Configure EAP-TLS on 9800 WLC with ISE Internal CA

Introduction

This document describes EAP-TLS authentication using the Certificate Authority of Identity Services Engine to authenticate users.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Wireless controller: C9800-40-K9 running 17.09.04a
- Cisco ISE: Running Version 3 Patch 4
- AP Model: C9130AXI-D
- Switch: 9200-L-24P

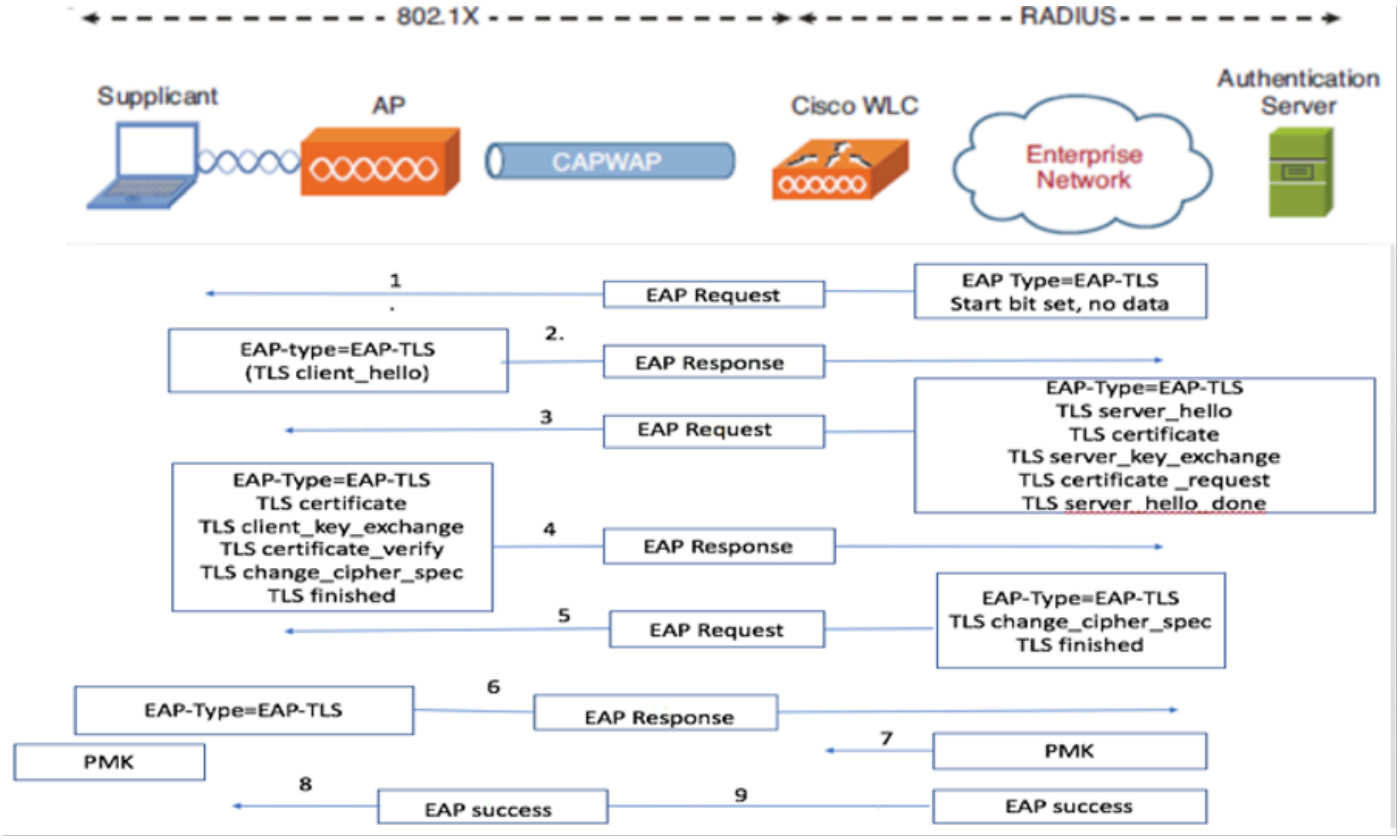
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Most organizations have their own CA that issues certificates to end users for EAP-TLS authentication. ISE includes an inbuilt certificate authority that can be used to generate certificates for users to be used in EAP-TLS authentication. In scenarios where using a full-fledged CA is not feasible, utilizing the ISE CA for user authentication becomes advantageous.

This document outlines the configuration steps required to effectively use the ISE CA to authenticate wireless users. EAP-TLS Authentication flow

EAP-TLS Authentication Flow



EAP-TLS Authentication Flow

Steps in the EAP-TLS Flow

1. The wireless client associates with the Access Point (AP).
2. At this stage, the AP does not permit data transmission and sends an authentication request.
3. The client, acting as the supplicant, responds with an EAP-Response Identity.

4. The Wireless LAN Controller (WLC) forwards the user ID information to the Authentication Server.
5. The RADIUS server replies to the client with an EAP-TLS Start Packet.
6. The EAP-TLS conversation begins from this point.
7. The client sends an EAP-Response back to the authentication server, including a client_hello handshake message with a cipher set to NULL.
8. The authentication server responds with an Access-Challenge packet containing:

```
TLS server_hello
Handshake message
Certificate
Server_key_exchange
Certificate request
Server_hello_done
```

9. The client replies with an EAP-Response message that includes:

```
Certificate (for server validation)
Client_key_exchange
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished
```

10. Upon successful client authentication, the RADIUS server sends an Access-Challenge containing:

```
Change_cipher_spec
Handshake finished message
```

11. The client verifies the hash to authenticate the RADIUS server.

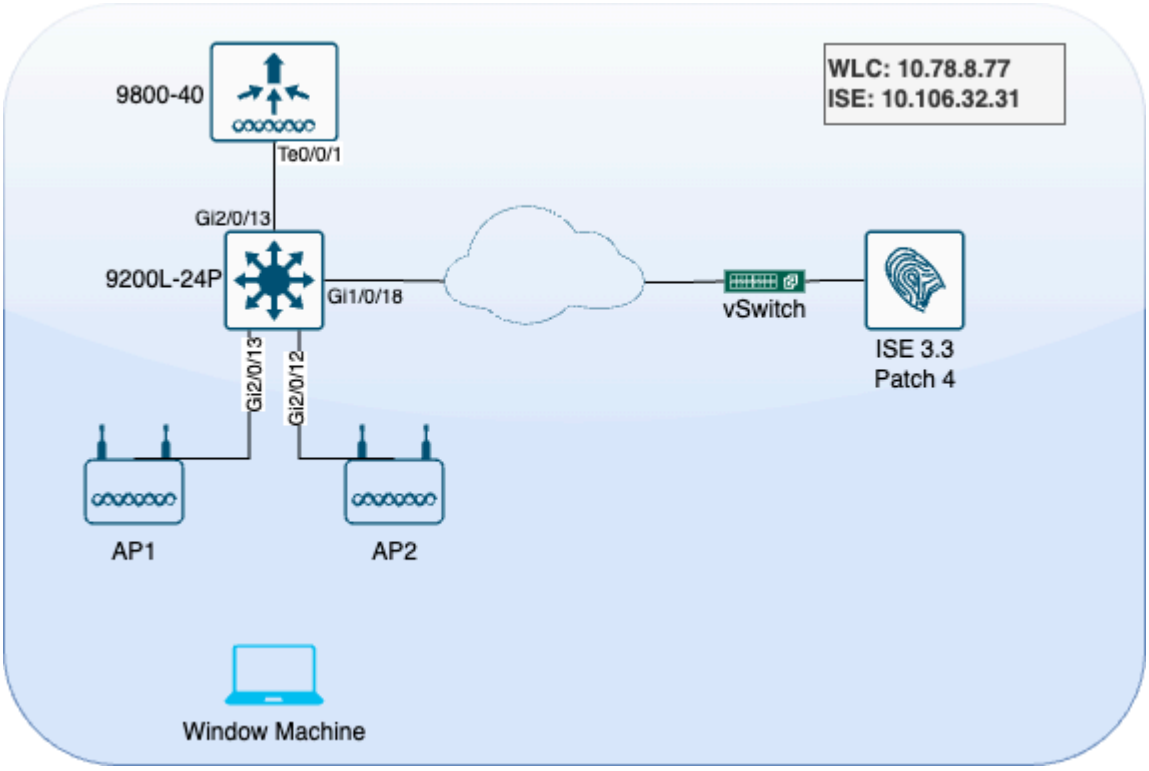
12. A new encryption key is dynamically derived from the secret during the TLS handshake.

13. An EAP-Success message is sent from the server to the authenticator and then to the supplicant.

14. The EAP-TLS enabled wireless client can now access the wireless network.

Configure

Network Diagram



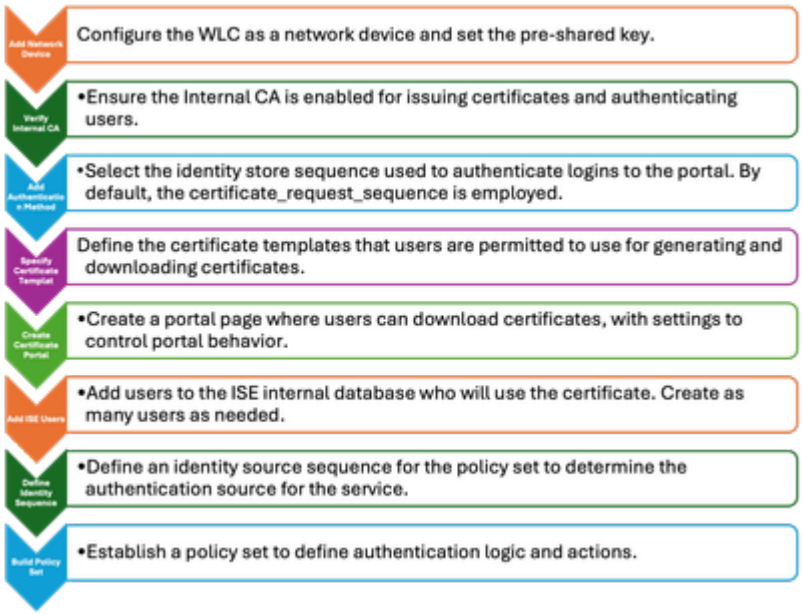
LAB Topology

Configurations

In this section, you configure two components: ISE and 9800 WLC.

ISE Configuration

Here are the configuration steps for the ISE server. Each step is accompanied by screenshots in this section to provide visual guidance.

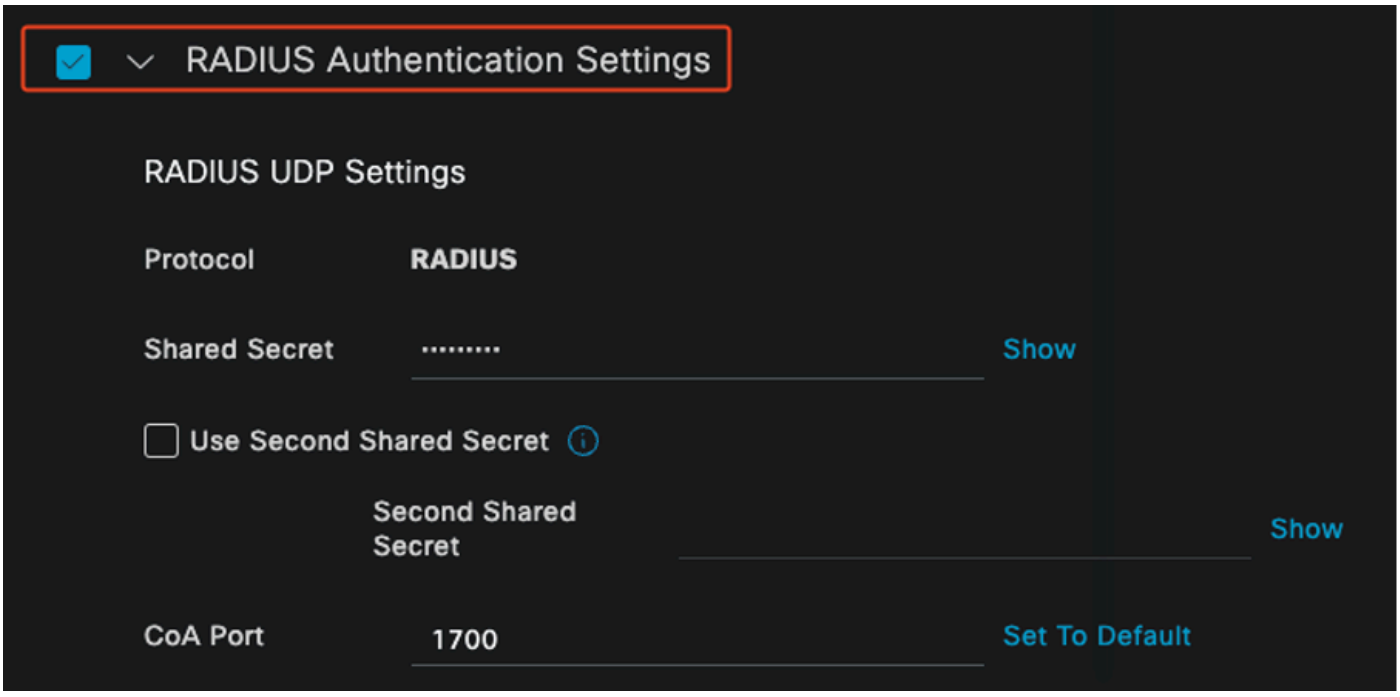


ISE Server Configuration Steps

Adding a Network Device

To add the Wireless LAN Controller (WLC) as a network device, use these instructions:

1. Navigate to **Administration > Network Resources > Network Devices**.
2. Click the **+Add** icon to initiate the process of adding the WLC.
3. Ensure that the pre-shared key matches both the WLC and the ISE server to enable proper communication.
4. Once all details are correctly entered, click **Submit** at the bottom left corner to save the configuration

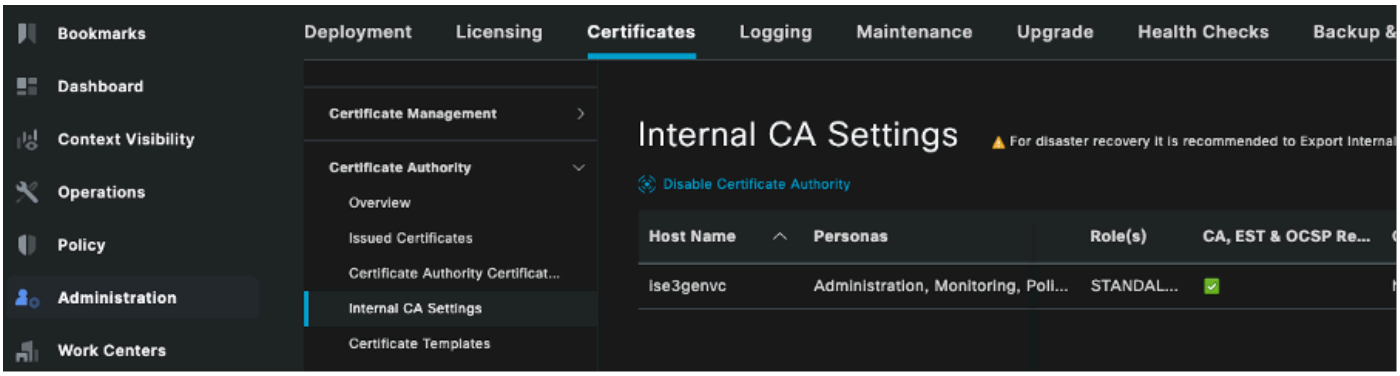


Adding a Network Device

Verify Internal CA

To verify the Internal Certificate Authority (CA) settings, use these steps:

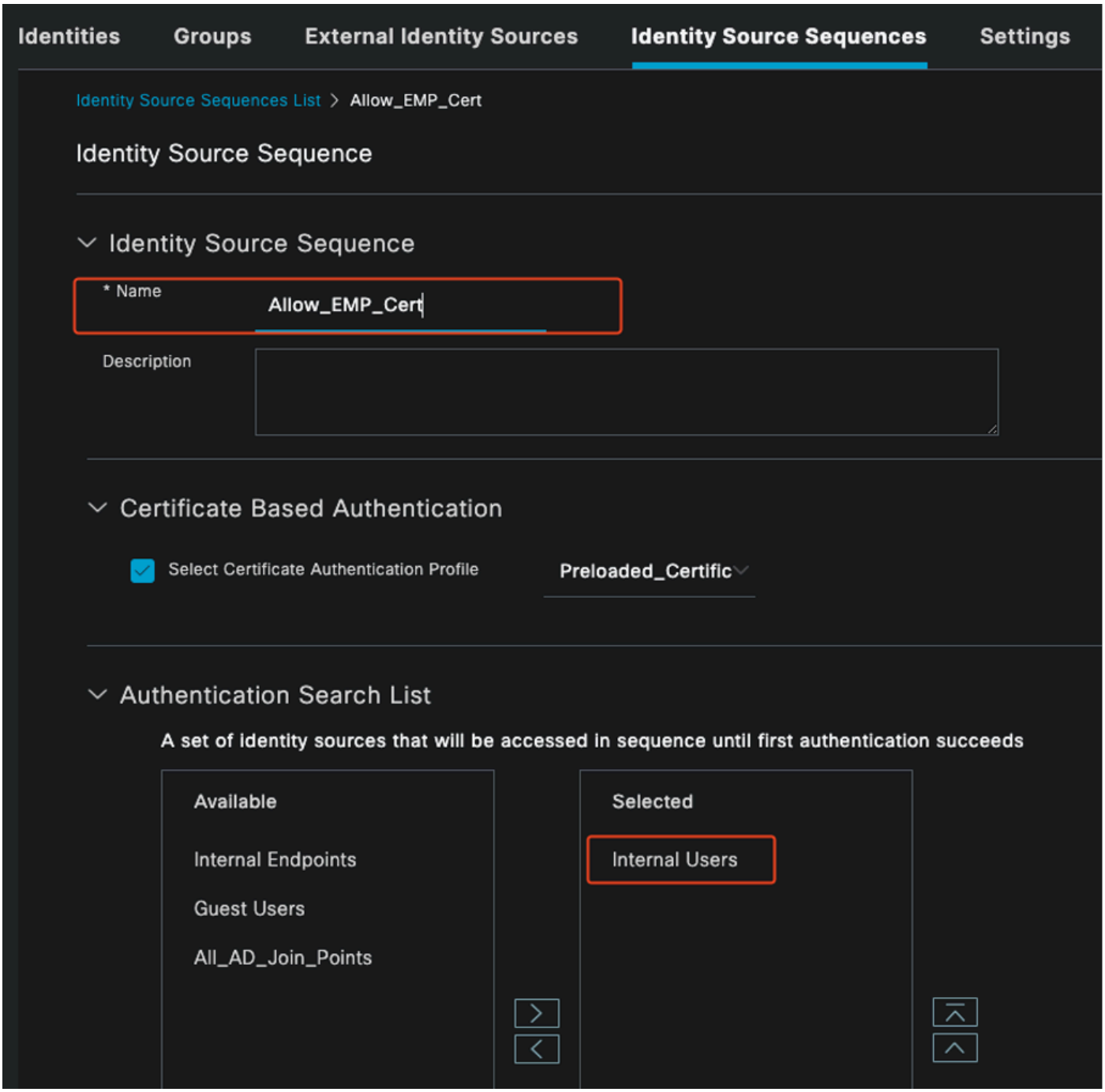
1. Navigate to **Administration > System > Certificates > Certificate Authority > Internal CA Settings**.
2. Ensure that the CA column is enabled to confirm that the internal CA is active.



Verify Internal CA

Add Authentication Method

Navigate to **Administration > Identity Management > Identity Source Sequences**. Add a **custom identity sequence** to control the portal log in source.



Authentication Method

Specify Certificate Template

To specify a certificate template, use these steps:

Step 1. Navigate to **Administration > System > Certificates > Certificate Authority > Certificate Templates**.

Step 2. Click the **+Add** icon to create a new certificate template:

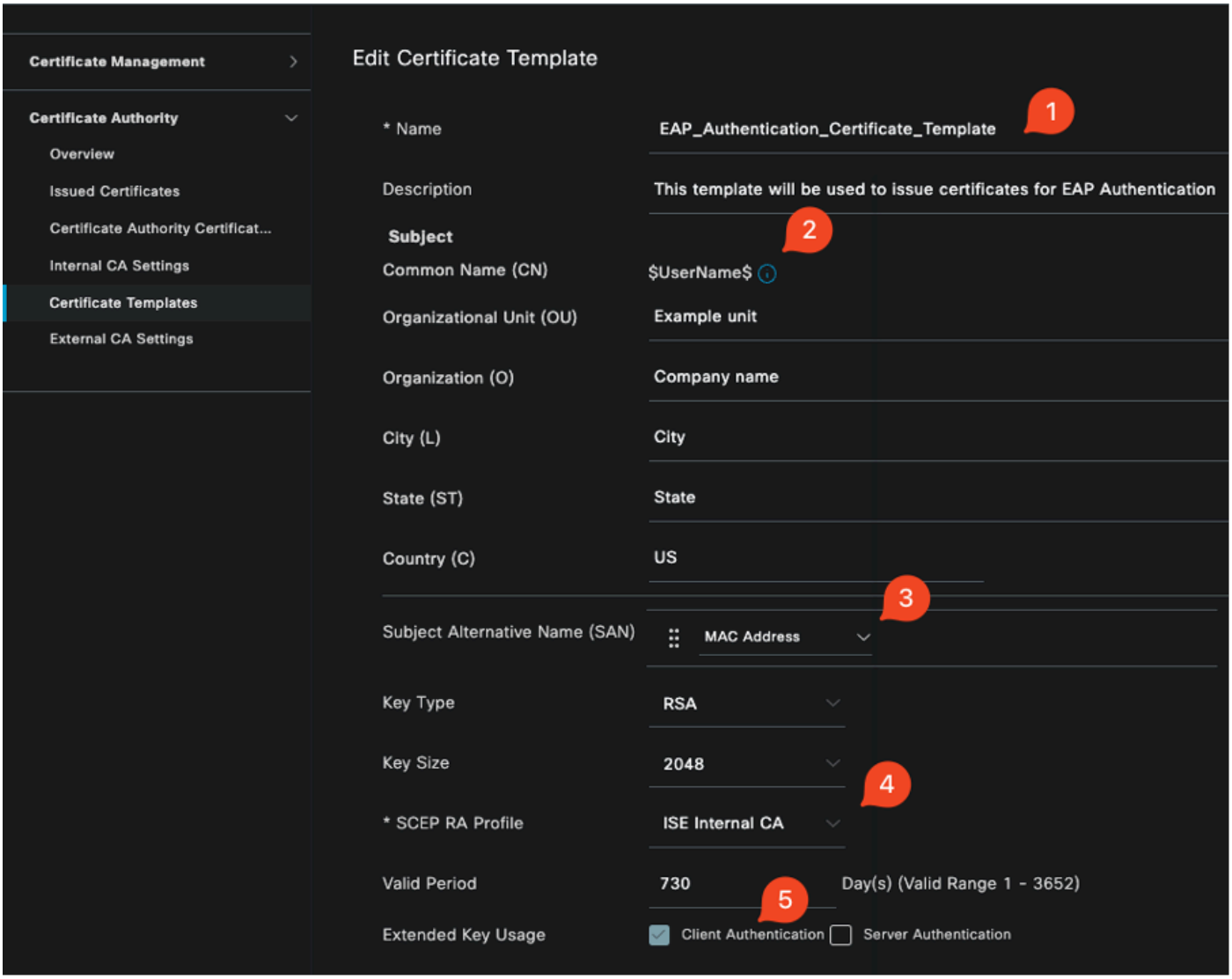
2.1 Provide a **unique name** that is local to the ISE server for the template.

2.2 Ensure the Common Name (CN) is set to $UserName$.

2.3 Verify that the Subject Alternative Name (SAN) is mapped to the MAC address.

2.4 Set the **SCEP RA profile** to **ISE Internal CA**.

2.5 In the extended key usage section, enable **client authentication**.



Certificate Template

Create Certificate Portal

To create a certificate portal for client certificate generation, use these steps:

Step 1. Navigate to **Administration > Device Portal Management > Certificate Provisioning**.

Step 2. Click **Create** to set up a new portal page.

Step 3. Provide a **unique name** for the portal to easily identify it.

3.1. Choose the **port number** for the portal to operate on; set this to 8443.

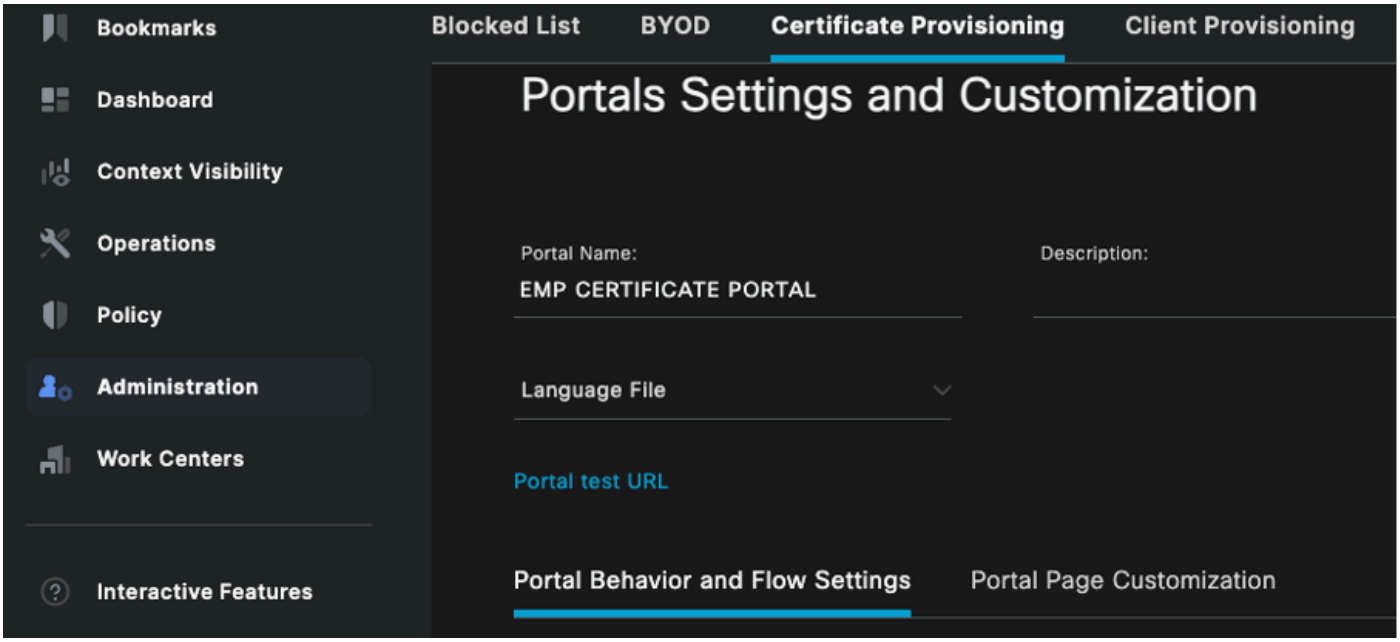
3.2. Specify the **interfaces** on which ISE listens for this portal.

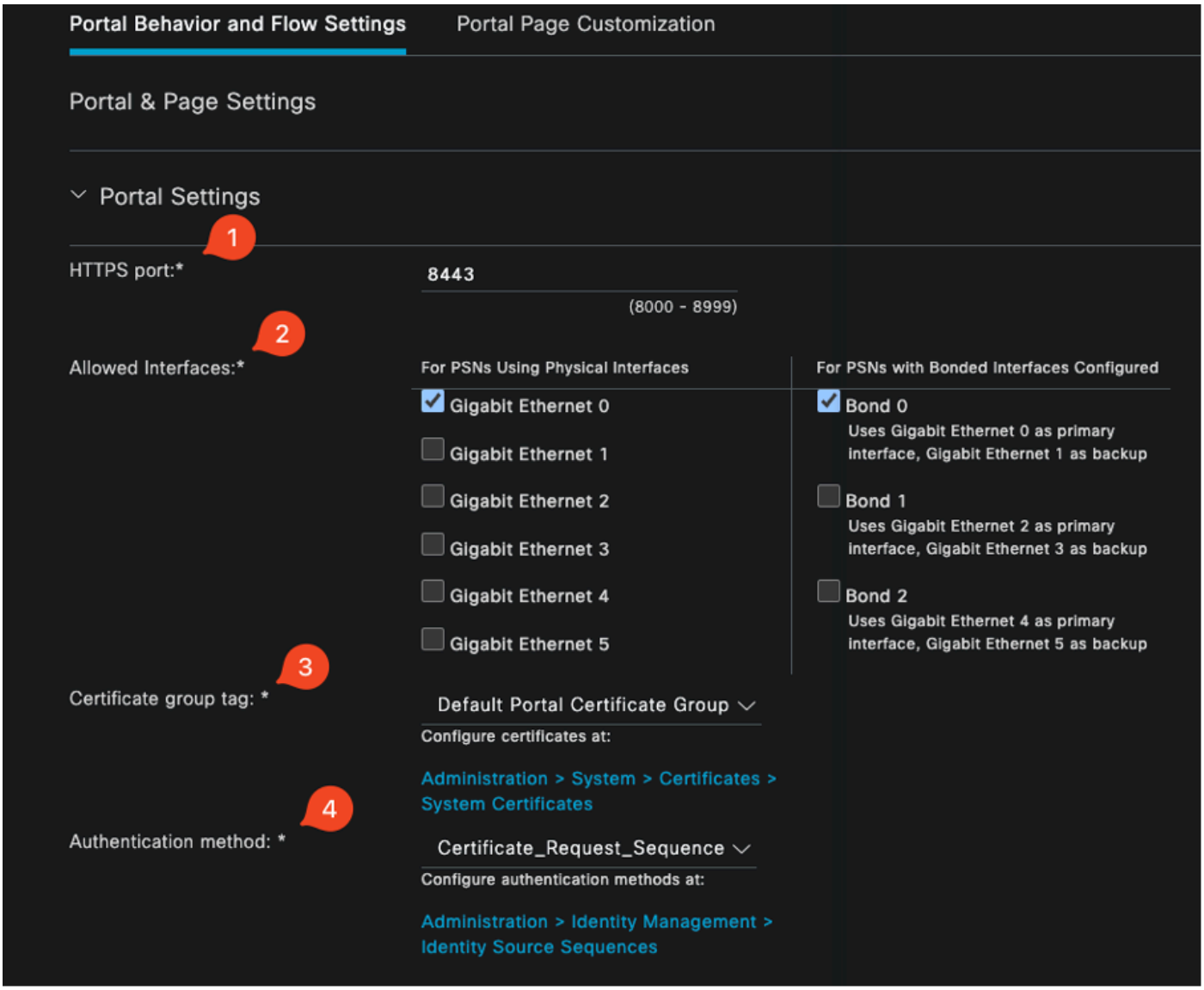
3.3. Select the **Certificate Group Tag** as the Default Portal Certificate Group.

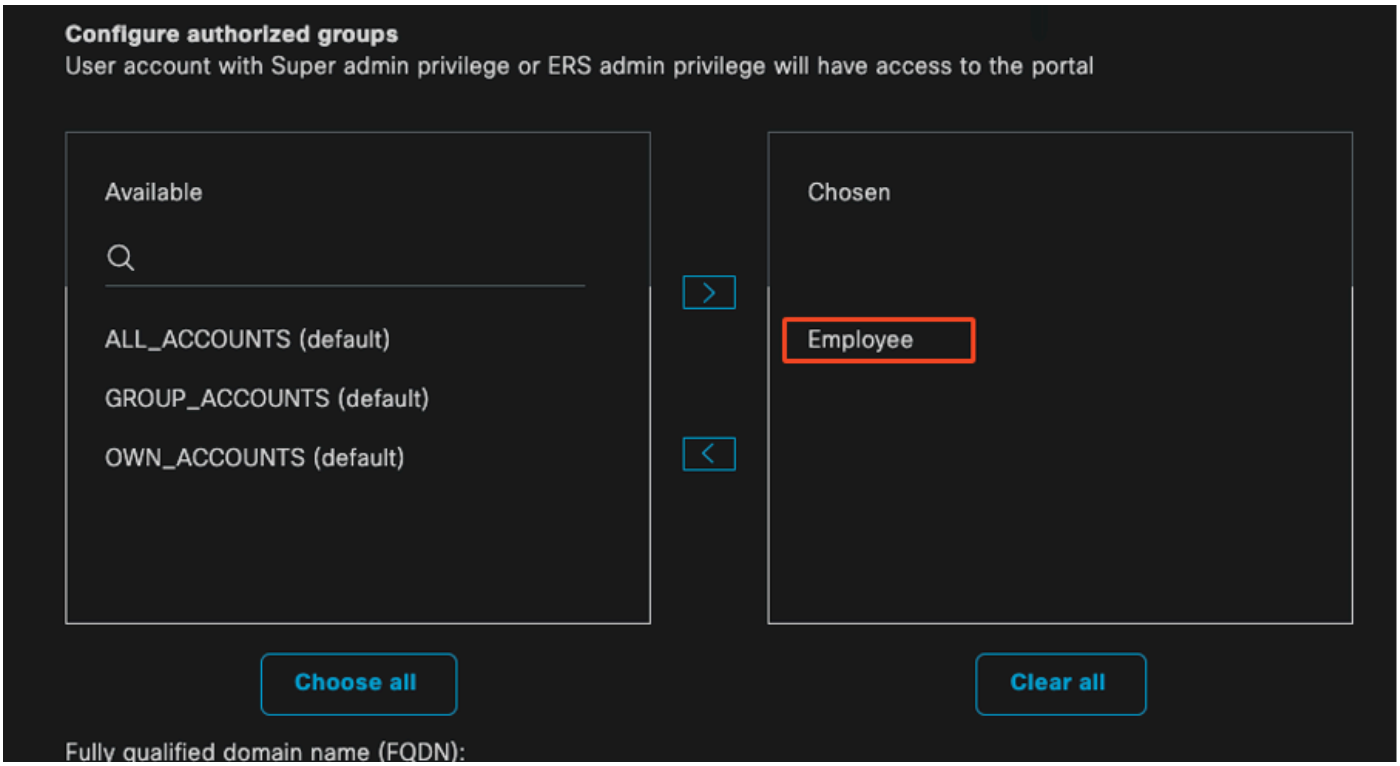
3.4. Select the **authentication method**, which indicates the identity store sequence used to authenticate log in to this portal.

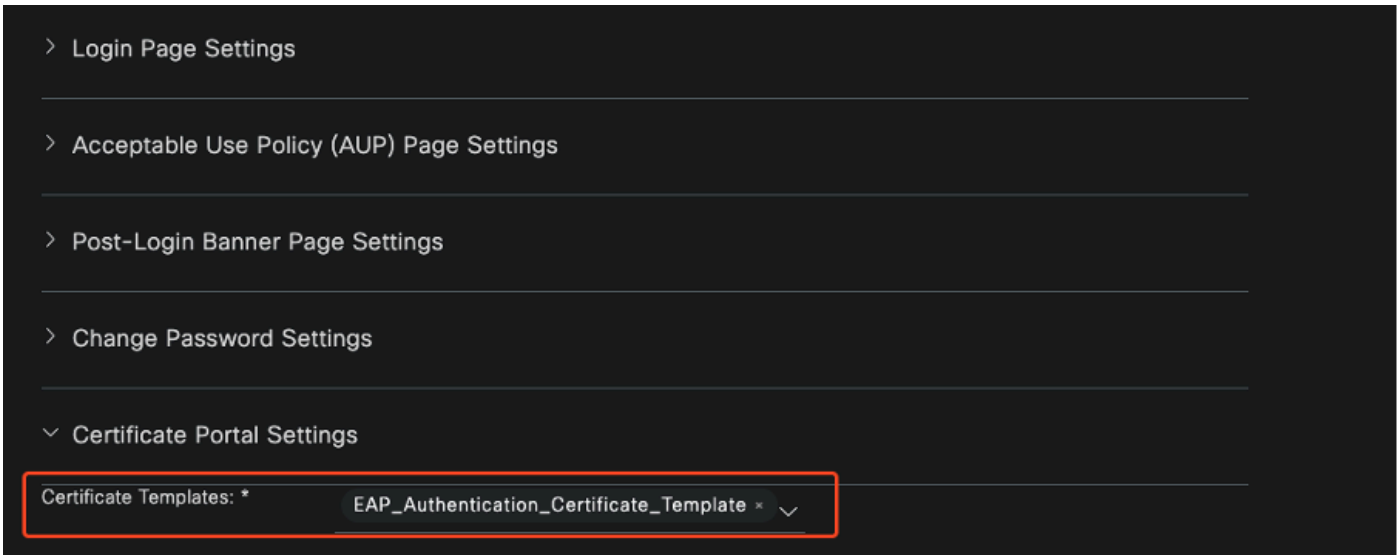
3.5. Include the **authorized groups** whose members can access the portal. For instance, select the **Employee** user group if your users belong to this group.

3.6. Define the **certificate templates** that are permitted under the Certificate Provisioning settings.



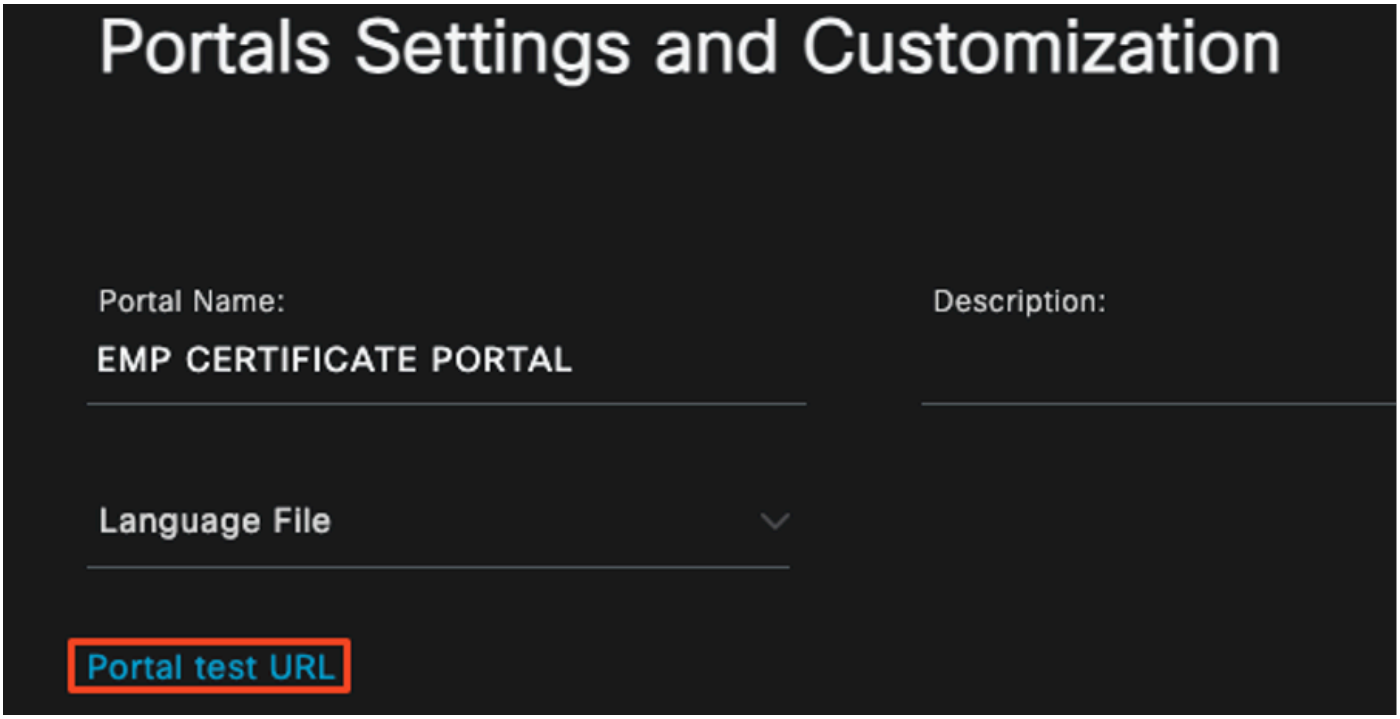

Portal Behavior and Flow Settings
Portal Page Customization
Portal & Page Settings
Portal Settings
1
HTTPS port:*
8443
(8000 - 8999)
2
Allowed Interfaces:*
For PSNs Using Physical Interfaces
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 5
For PSNs with Bonded Interfaces Configured
Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup
3
Certificate group tag: *
Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates
4
Authentication method: *
Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences


Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal
Available
ALL_ACCOUNTS (default)
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)
Chosen
Employee
Choose all
Clear all
Fully qualified domain name (FQDN):

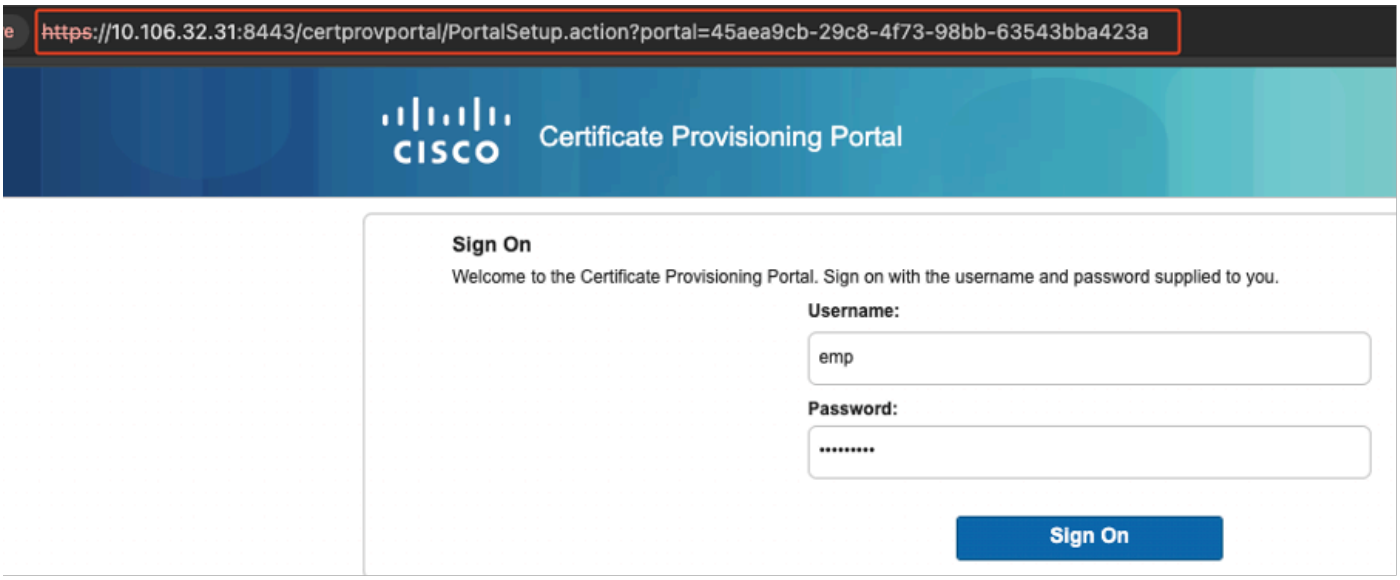


Certificate Portal Configuration

Once this setup is completed, you can test the portal by clicking the **Portal Test URL**. This action opens the portal page.



Test Portal Page URL

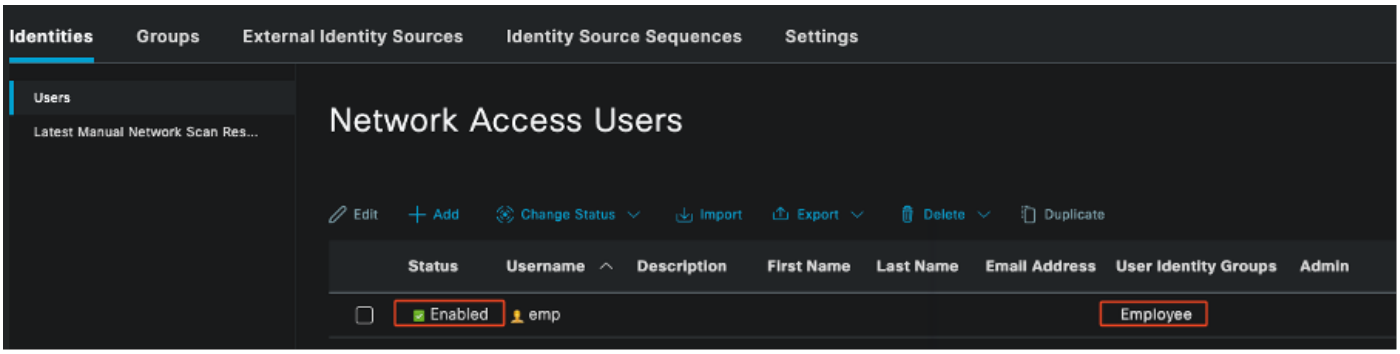


Portal Page

Add Internal User

To create a user for authenticating via the certificate portal, use these steps:

1. Navigate to **Administration > Identity Management > Identities > Users**.
2. Click the option to add a **user** to the system.
3. Select the **User Identity Groups** that the user belongs to. For this example, assign the user to the **Employee** group.



Adding Internal User

ISE Certificate Provisioning Portal and RADIUS Policy Configuration

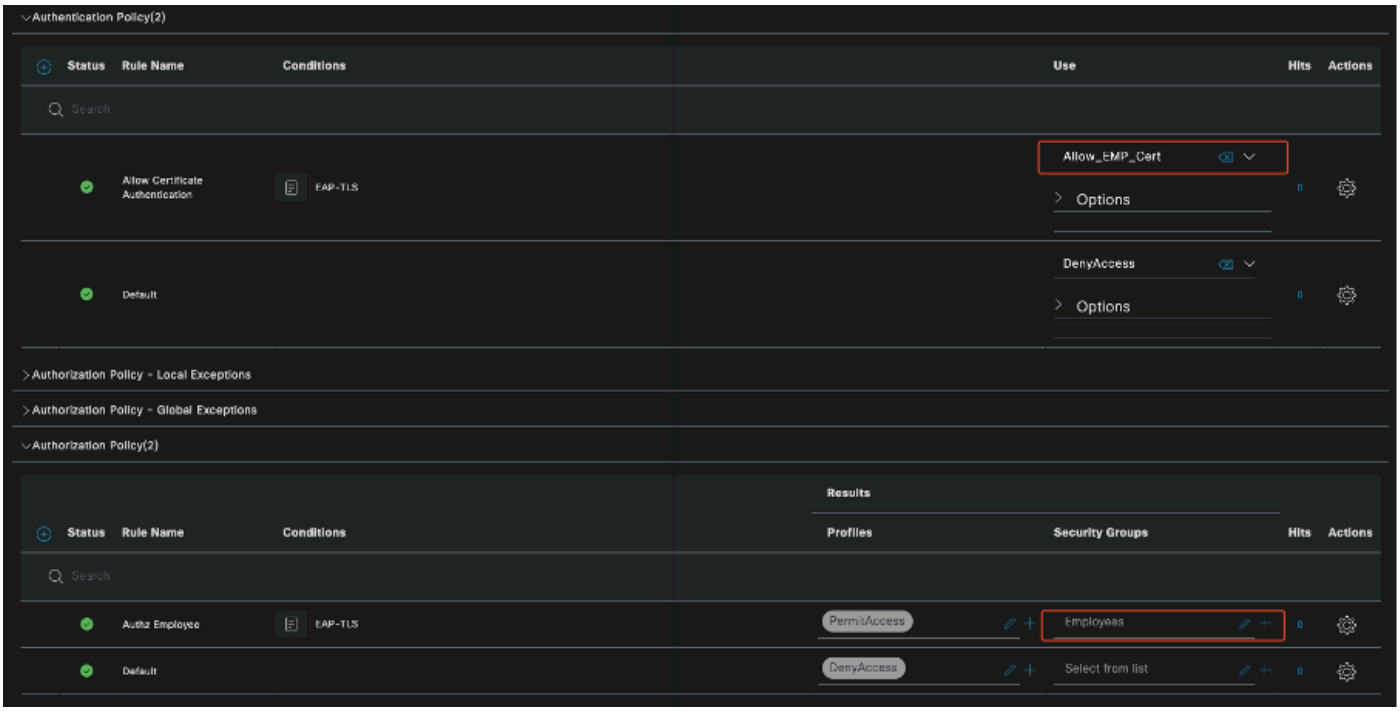
The previous section covered the setup of the ISE certificate provisioning portal. Now, you configure the ISE RADIUS policy sets to allow user authentication.

1. Configure **ISE RADIUS Policy Sets**.
2. Navigate to **Policy > Policy Sets**.
3. Click the **plus sign (+)** to create a new policy set.

In this example, set up a **simple policy set** designed to authenticate users using their certificates.



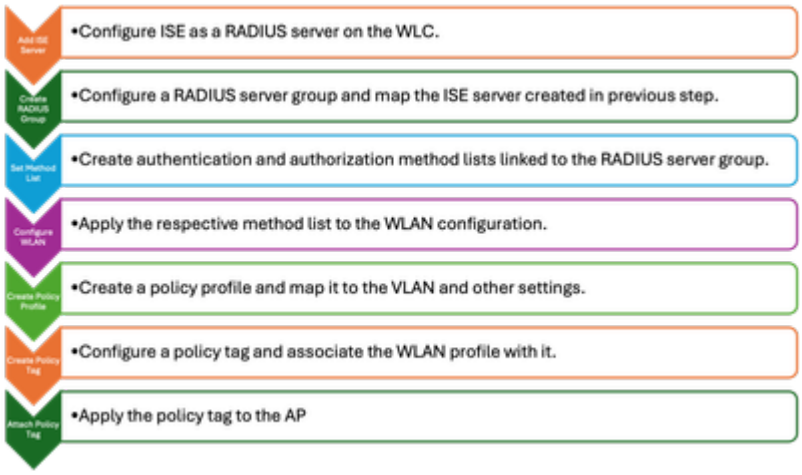
Policy Set



Policy Set Showing Authentication and Authorization Policies

9800 WLC configuration

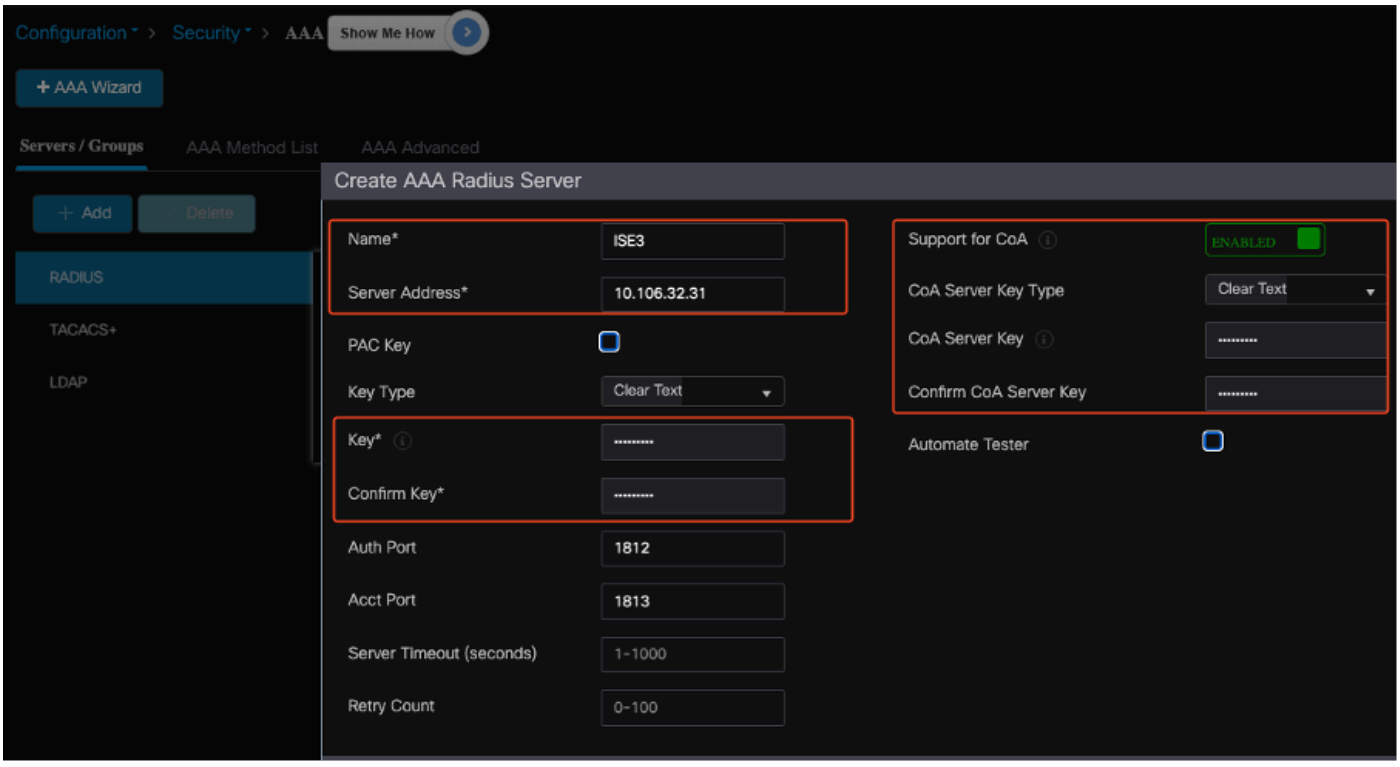
Here are the configuration steps for the 9800 WLC. Each step is accompanied by screenshots in this section to provide visual guidance.



WLC Configuration Steps

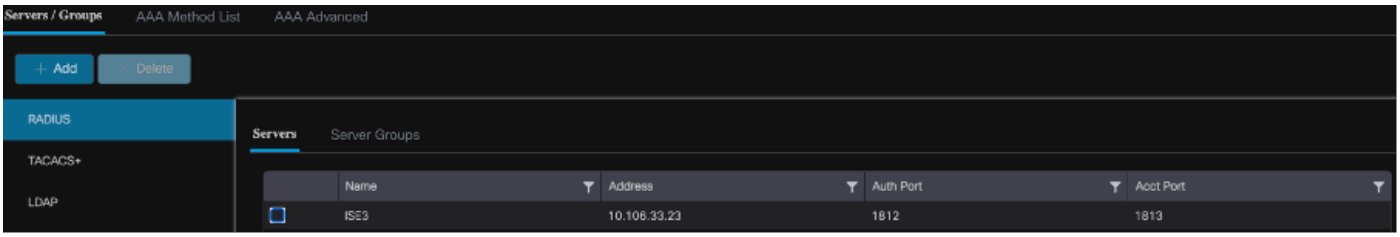
Add ISE Server to 9800 WLC

1. To integrate the ISE server with the 9800 Wireless LAN Controller (WLC), use these steps:
2. Navigate to **Configuration > Security > AAA**.
3. Click the **Add** button to include the ISE server in the WLC configuration.



Adding ISE Server In the WLC

Once the server is added, it appears in the list of servers.

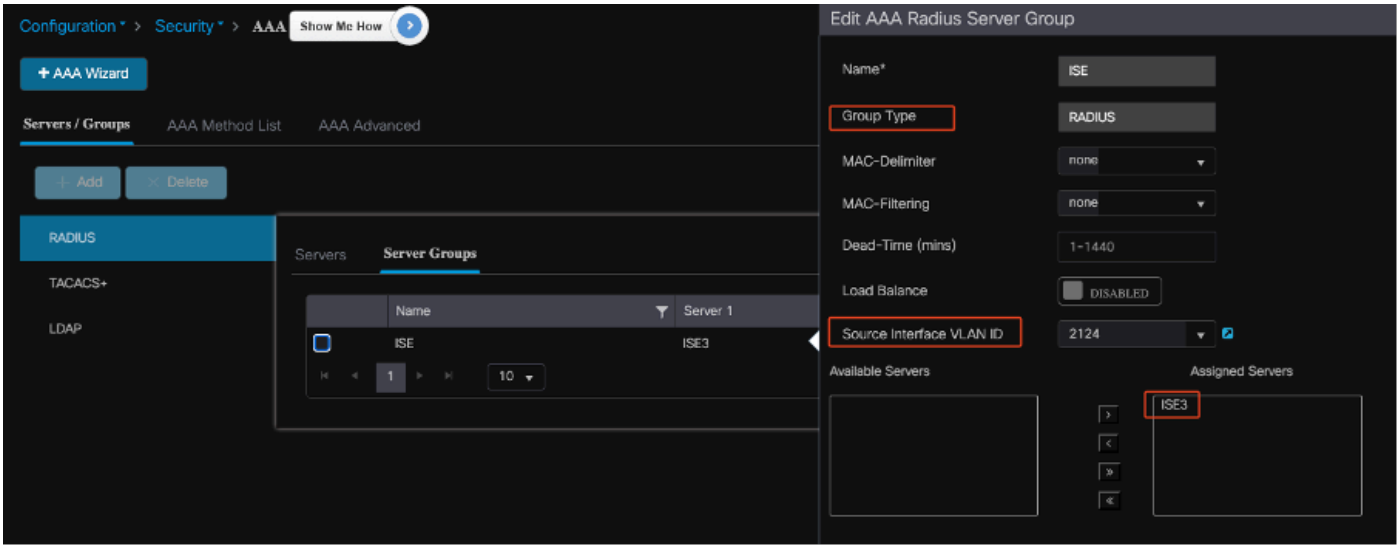


Showing Radius Servers

Add Server Group on 9800 WLC

To add a server group on the 9800 Wireless LAN Controller, complete these steps:

1. Navigate to **Configuration > Security > AAA**.
2. Click the **Server Group** tab, then click **Add** to create a new server group.

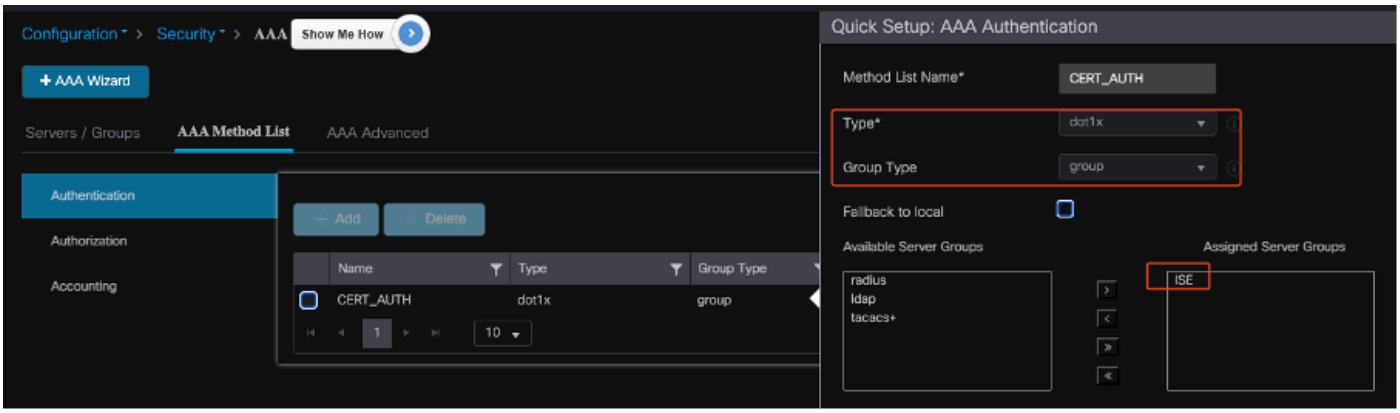


Mapping ISE Servers to a Radius Server Group

Configure AAA Method List on 9800 WLC

After creating the server group, configure the authentication method list using these steps:

1. Navigate to **Configuration > Security > AAA > AAA Method List**.
2. In the Authentication tab, add a **new authentication method list**.
3. Set the type to **dot1x**.
4. Select **group** as the group type.
5. Include the **ISE server groups** that you created earlier as the server groups.

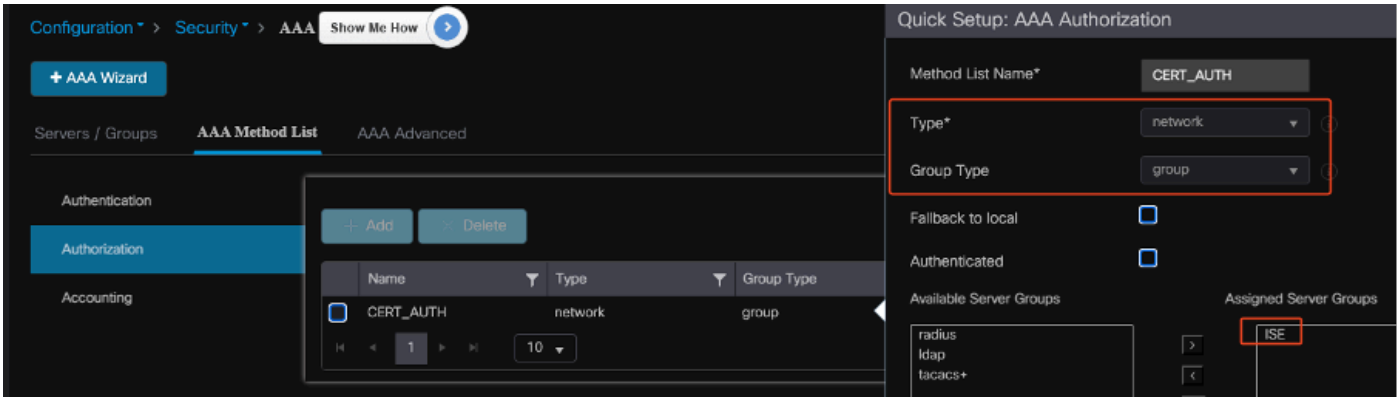


Creating Authentication Method Lists

Configure Authorization Method List on 9800 WLC

To set up the authorization method list, use these steps:

1. Navigate to the **Authorization tab** within the AAA Method List section.
2. Click **Add** to create a new authorization method list.
3. Choose **network** as the type.
4. Select **group** as the group type.
5. Include the **ISE server group** as the server group.

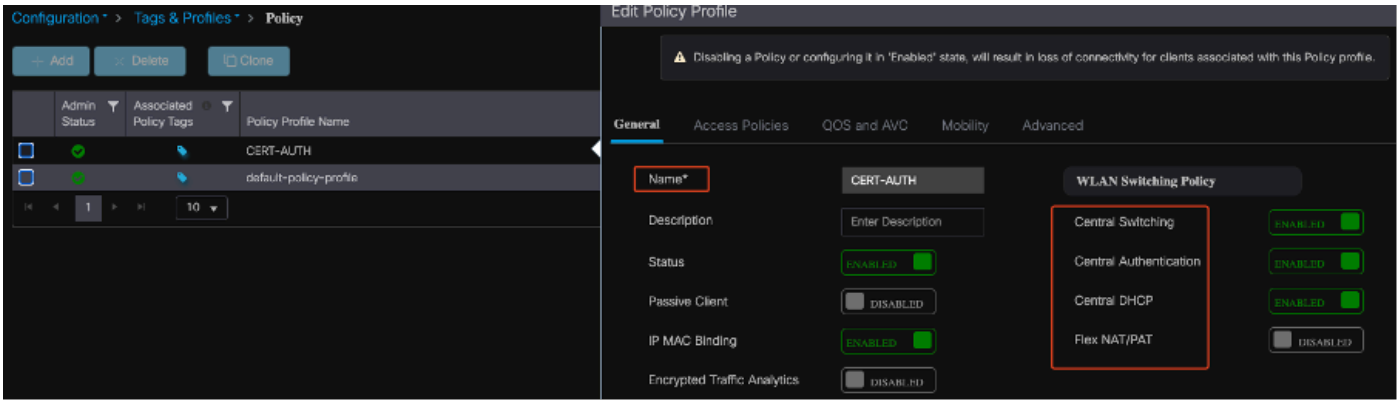


Adding Authorization Method List

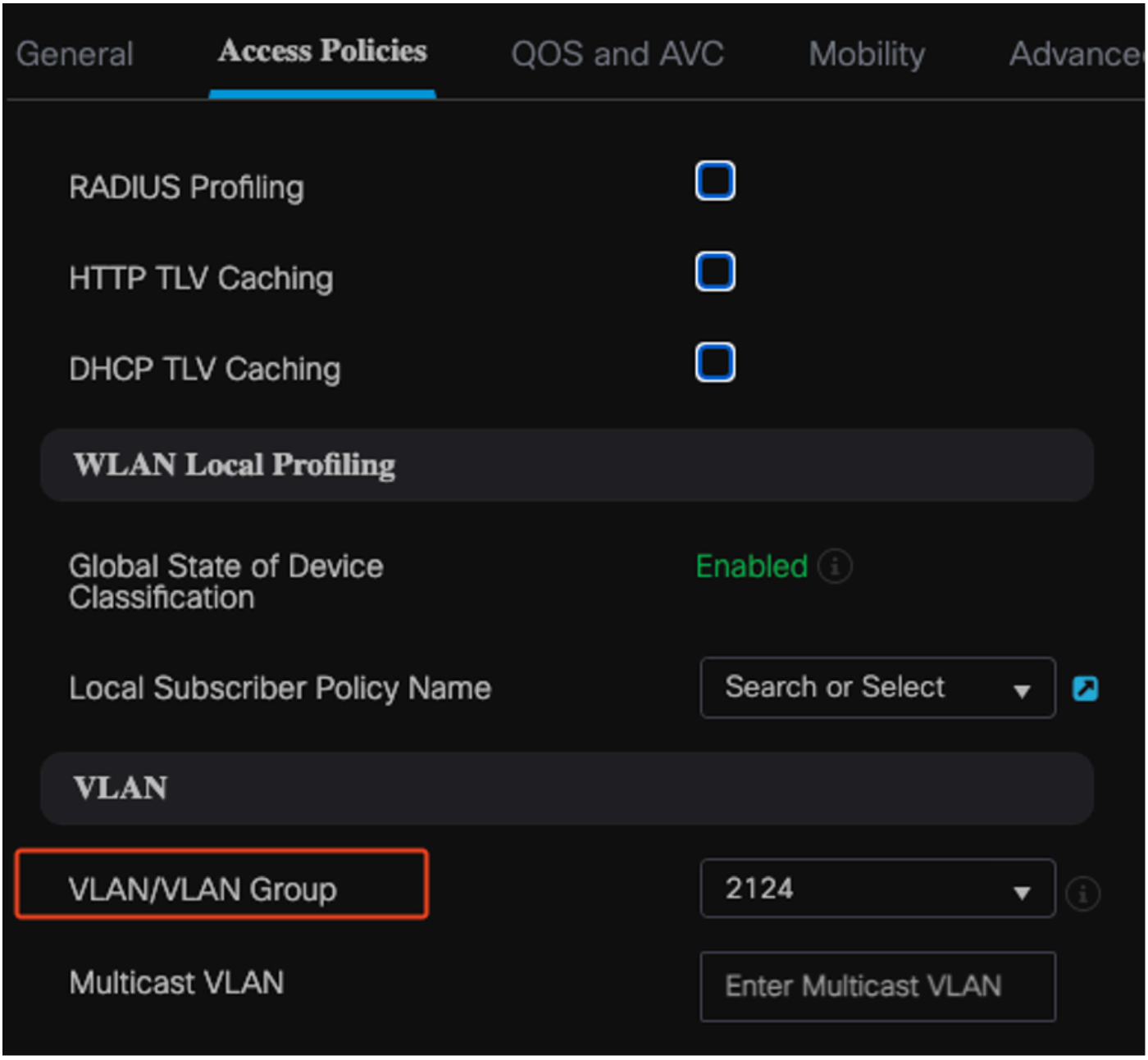
Create a Policy Profile on 9800 WLC

With the RADIUS group configuration complete, proceed to create a policy profile:

1. Navigate to **Configuration > Tags & Profiles > Policy.**
2. Click **Add** to create a new policy profile.
3. Choose the appropriate parameters for your policy profile. In this example, everything is central and **LAB VLAN** is used as the client VLAN.



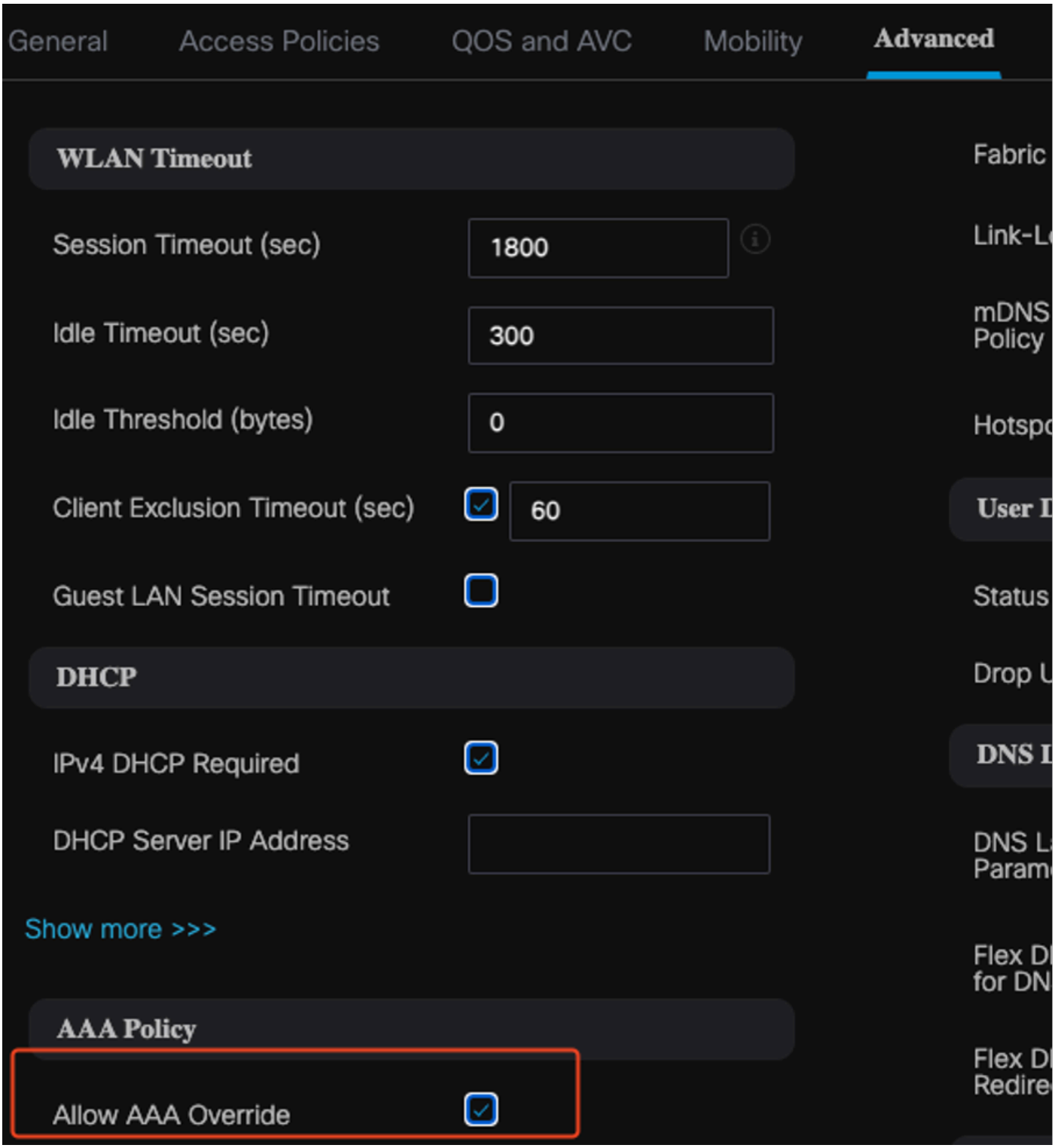
Configuring Policy Profile



VLAN to Policy Mapping

When configuring RADIUS authorization, ensure that the **AAA Override** option is enabled in the advanced

tab of the policy profile settings. This setting allows the Wireless LAN Controller to apply RADIUS-based authorization policies to users and devices.

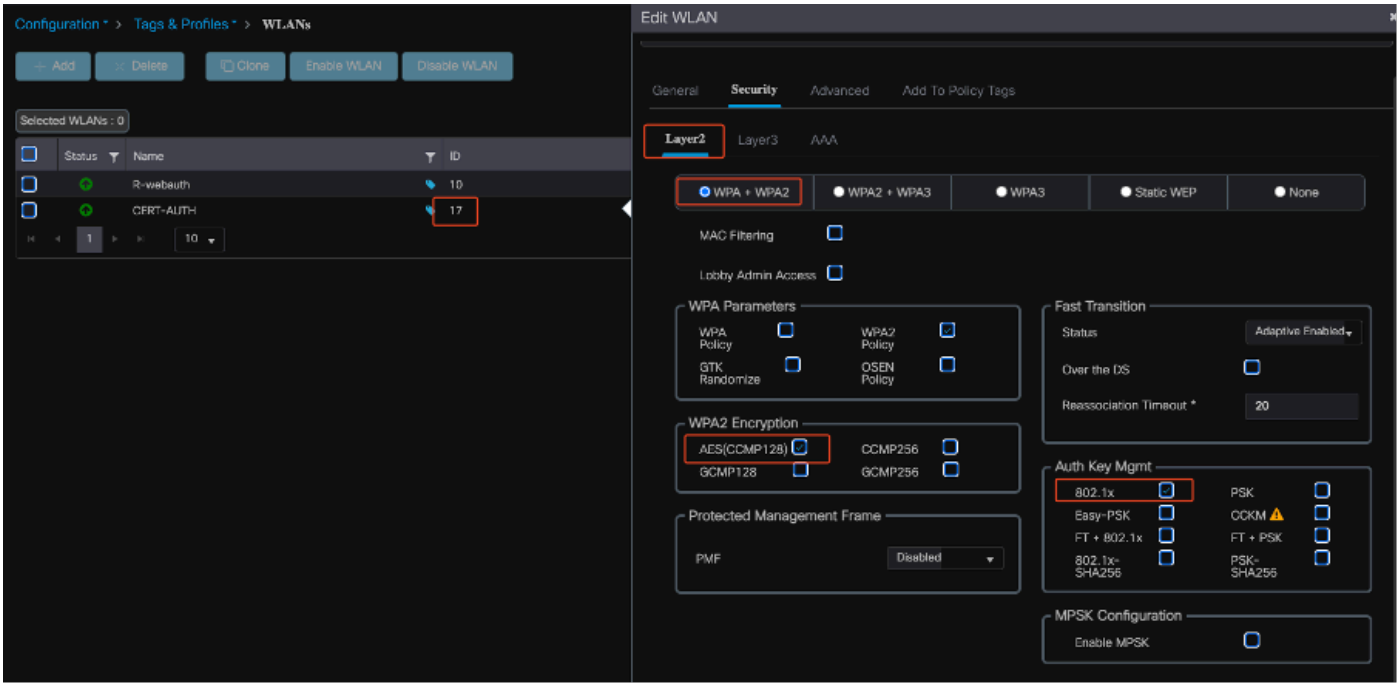


AAA Override

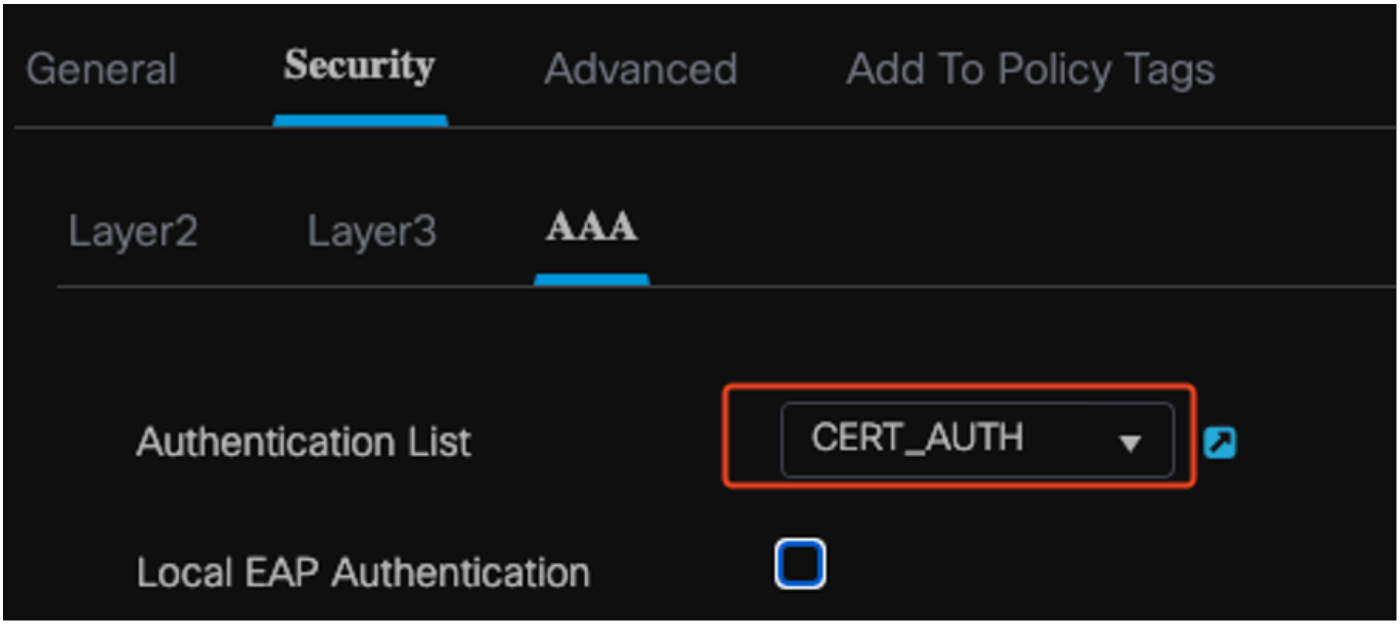
Create a WLAN on 9800 WLC

To set up a new WLAN with 802.1x authentication, use these steps:

1. Navigate to **Configuration > Tags & Profiles > WLANs**.
2. Click **Add** to create a new WLAN.
3. Select the **Layer 2 authentication** settings and enable **802.1x authentication**.



WLAN Profile configuration



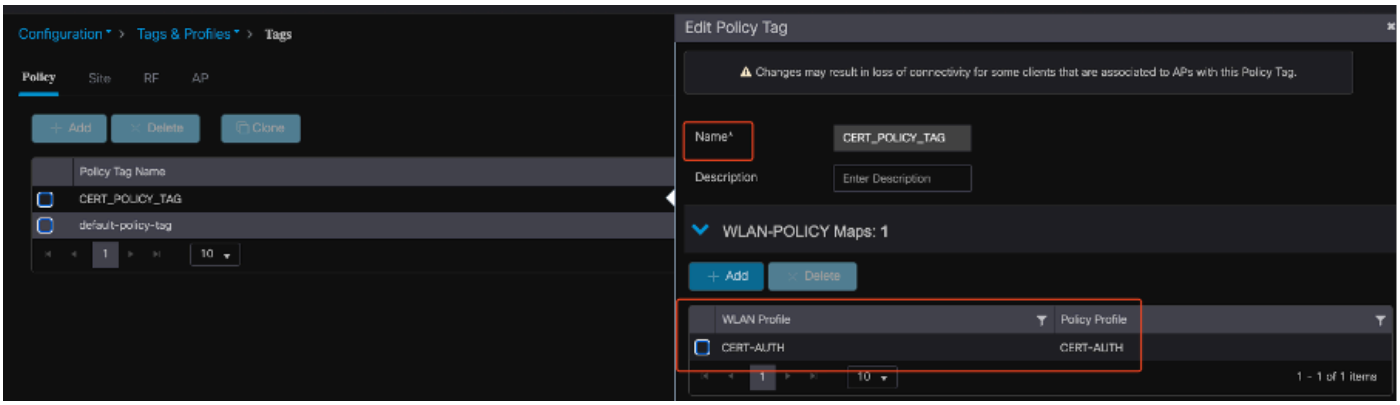
WLAN Profile to Method List Map

Map WLAN with Policy Profile on 9800 WLC

To associate your WLAN with a policy profile, use these steps:

1. Navigate to **Configuration > Tags & Profiles > Tags**.

2. Click **Add** to add a new tag.
3. In the WLAN-POLICY section, map the **newly created WLAN** to the appropriate policy profile.

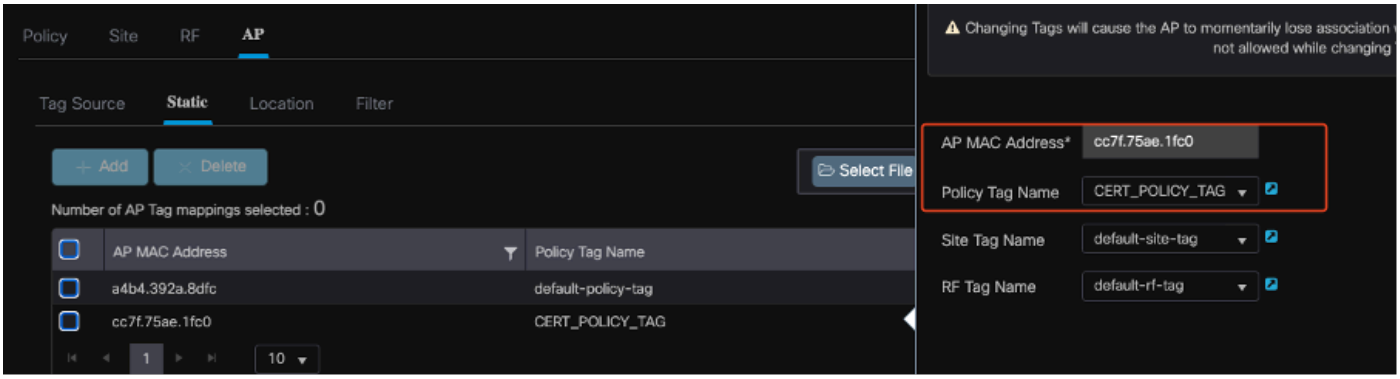


Policy TAG Configuration

Map Policy Tag to Access Point on 9800 WLC

To assign the policy tag to an Access Point (AP), complete these steps:

1. Navigate to **Configuration > Tags & Profiles > Tags > AP**.
2. Navigate to the **Static** section within the AP configuration.
3. Click the specific **AP** you want to configure.
4. Assign the **policy tag** you created to the selected AP.



AP TAG Assignment

Running Configuration of the WLC After Setup Completion

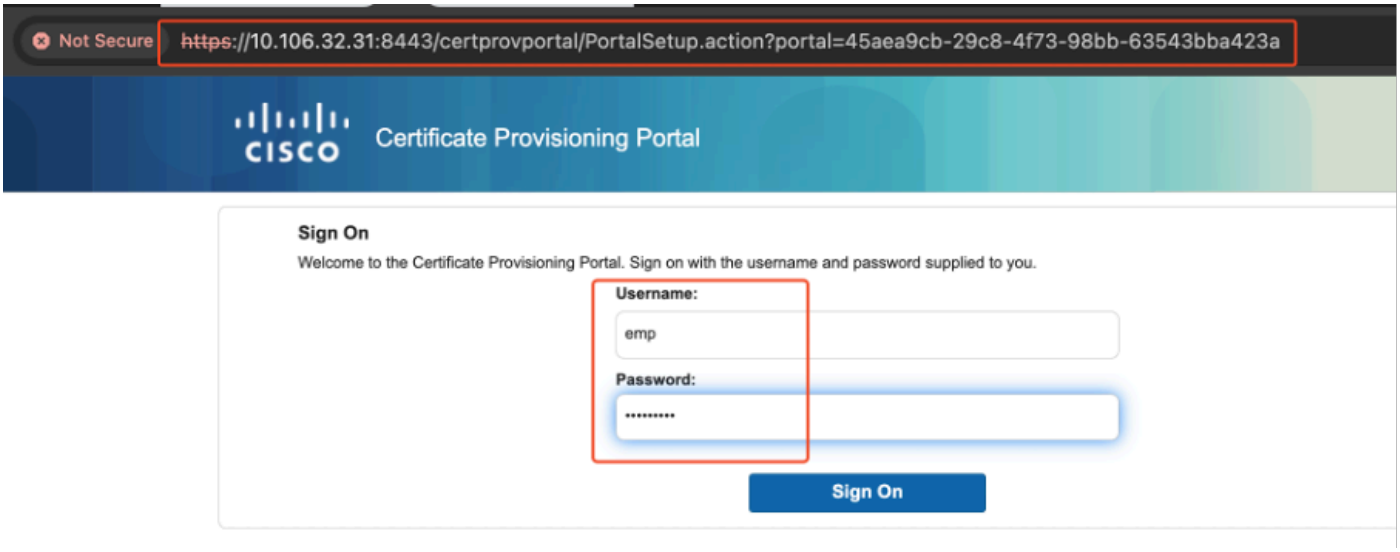
```
aaa group server radius ISE
 server name ISE3
 ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
 client 10.106.32.31 server-key Cisco!123
!
```

```
wireless profile policy CERT-AUTH
 aaa-override
 ipv4 dhcp required
 vlan 2124
 no shutdown
 wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
 security dot1x authentication-list CERT_AUTH
 no shutdown
!
wireless tag policy CERT_POLICY_TAG
 wlan CERT-AUTH policy CERT-AUTH
```

Create and Download Certificate for the User

To create and download a certificate for a user, navigate through these steps:

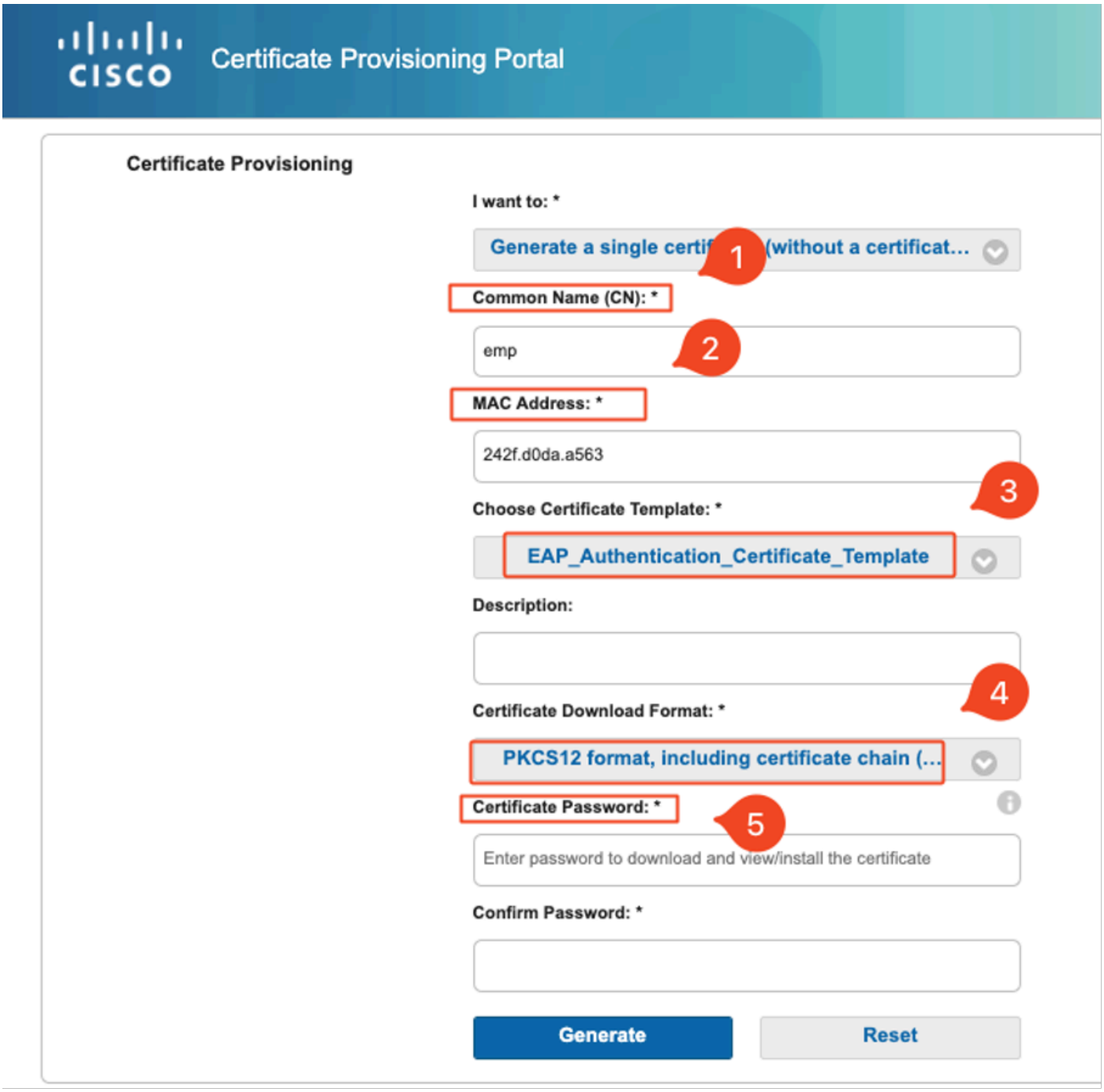
1. Have the user log into the certificate portal that was set up earlier.



Accessing Certificate Portal

2. Accept the Acceptable Use Policy (AUP). The ISE then presents a page for certificate generation.

3. Select **Generate a single certificate (without a certificate signing request)**.



Generating Certificate

To generate a certificate via the Certificate Provisioning Portal, ensure that these mandatory fields are completed:

- CN: The authentication server uses the value that is presented in the Common Name field in the client certificate to authenticate a user. In the Common Name field, enter the **username** (that you used to log in to the Certificate Provisioning Portal).
- MAC Address: Subject Alternative Names (SAN) is an X.509 extension that allows various values to be associated with a security certificate. Cisco ISE, Release 2.0 supports MAC address only. Hence, in the SAN/MAC address field.
    - Certificate Template: The certificate template defies a set of fields that the CA uses when validating a request and issuing a certificate. Fields such as the Common Name (CN) are used to validate the request (CN must match the username)). Other fields are used by the CA while

issuing the certificate.

- Certificate Password: You need a certificate password to secure your certificate. You must supply the certificate password to view the contents of the certificate and to import the certificate on a device.
- Your password must conform to these rules:
- Password must contain at least 1 uppercase letter, 1 lowercase letter, and 1 digit
    - Password must be between 8 and 15 characters long
    - Allowed characters include A-Z, a-z, 0-9, _, #

Once all fields are filled out, select **Generate** to create and download the certificate.

Certificate Installation on a Windows 10 Machine

To install a certificate on a Windows 10 machine, open the Microsoft Management Console (MMC) using these steps:

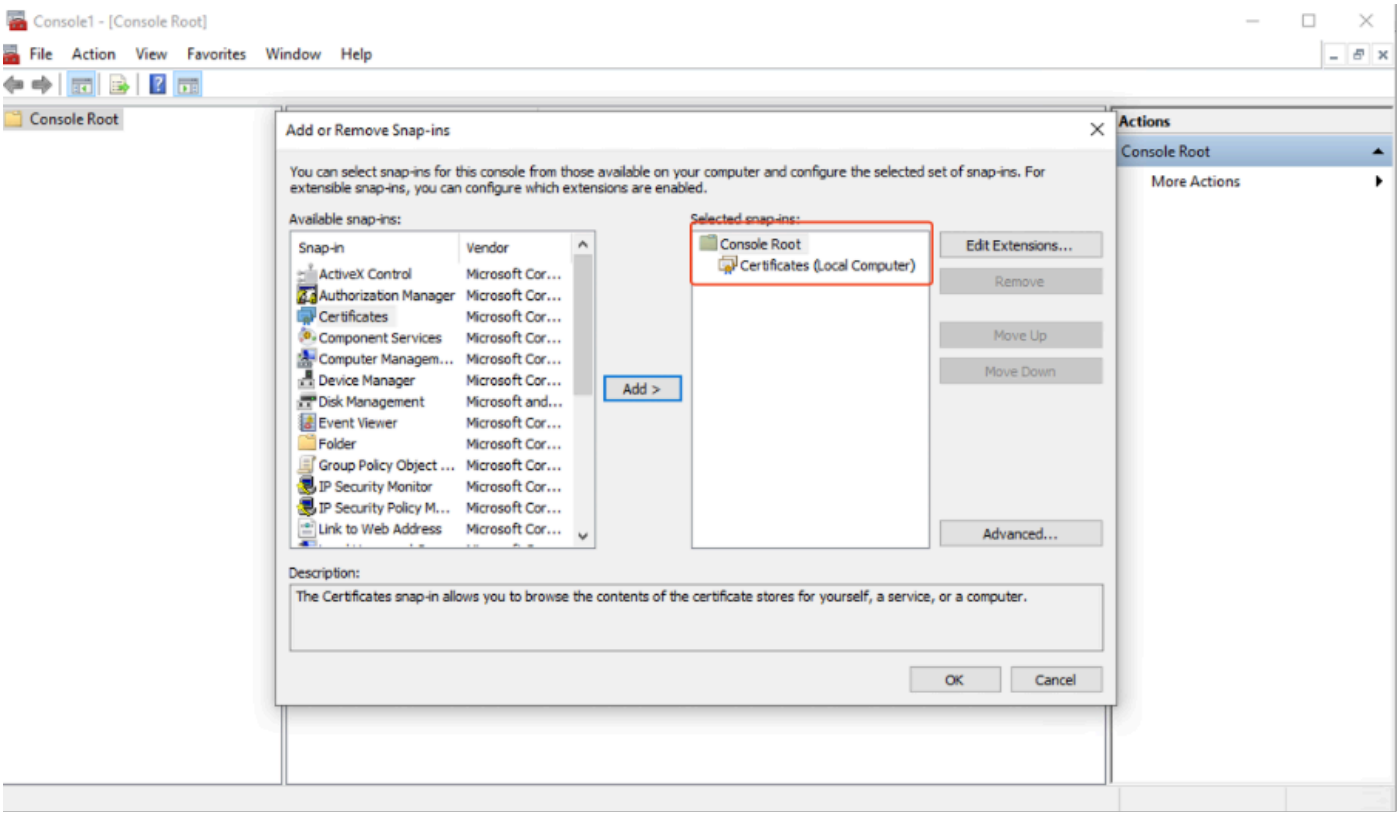


Note: These instructions can vary based on your Windows setup, so consulting the Microsoft documentation for specific details is recommended.

---

1. Click **Start** and then **Run**.
2. Type **MMC** in the Run box and press **Enter**. The Microsoft Management Console opens.
3. Add **Certificate** Snap-In:
4. Navigate to **File > Add/Remove Snap-In**.
5. Select **Add**, then choose **Certificates** and click **Add**.
6. Select **Computer Account**, then **Local Compute**r, and click **Finish**.

These steps allow you to manage certificates on your local computer.



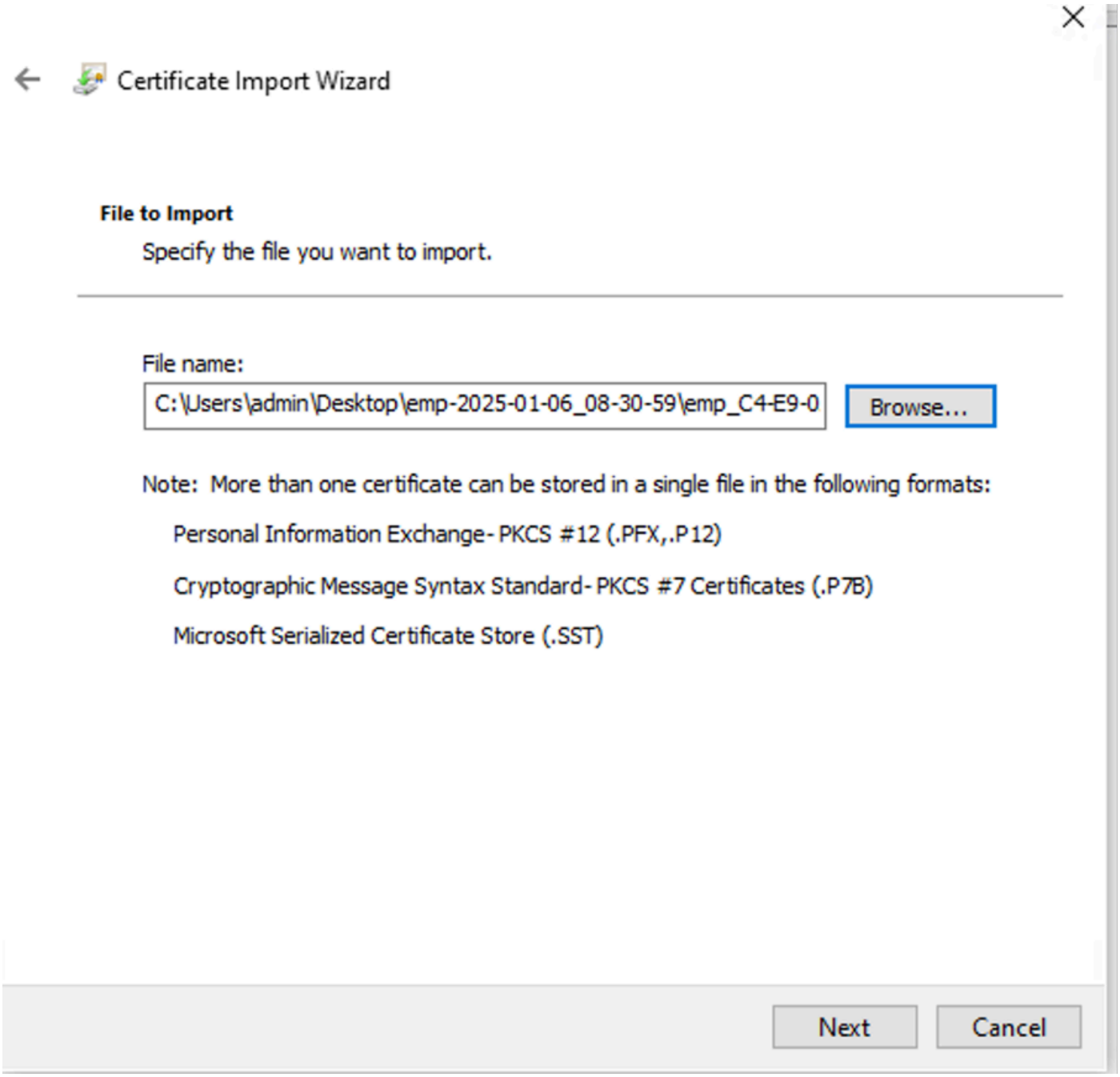
Windows MMC Console

Step 1. Import the Certificate:

1.1. Click **Action** in the menu.

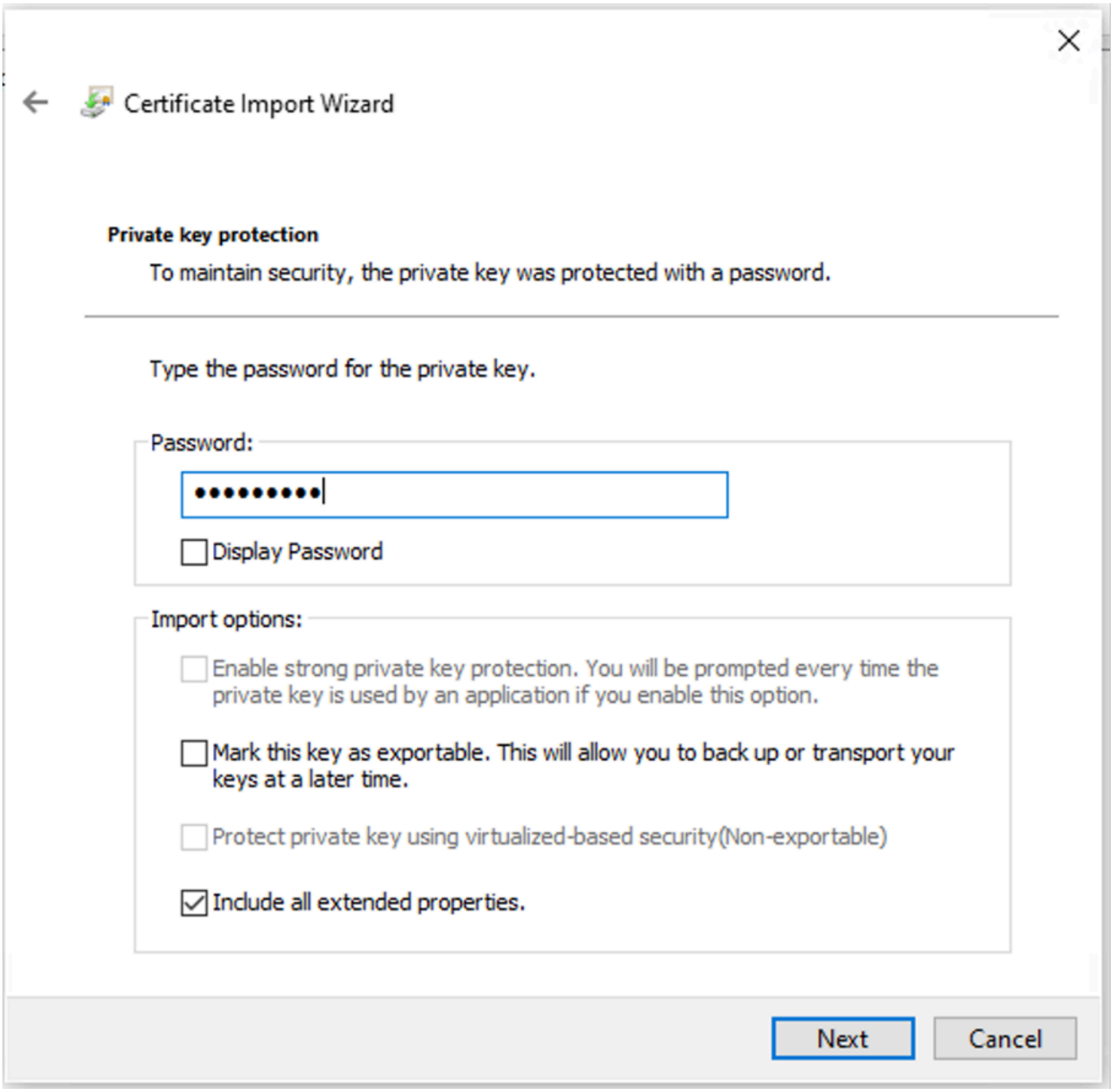
1.2. Navigate to **All Tasks**, then select **Import**.

1.3. Proceed through the prompts to locate and select the certificate file stored on your machine.



Importing Certificate

During the certificate import process, you are prompted to enter the password you created when generating the certificate on the portal. Ensure you enter this password accurately to successfully import and install the certificate on your machine.



Entering Certificate Password

Step 2. Move Certificates to Appropriate Folders:

2.1. Open the **Microsoft Management Console (MMC)** and navigate to the **Certificates (Local Computer) > Personal folder**.

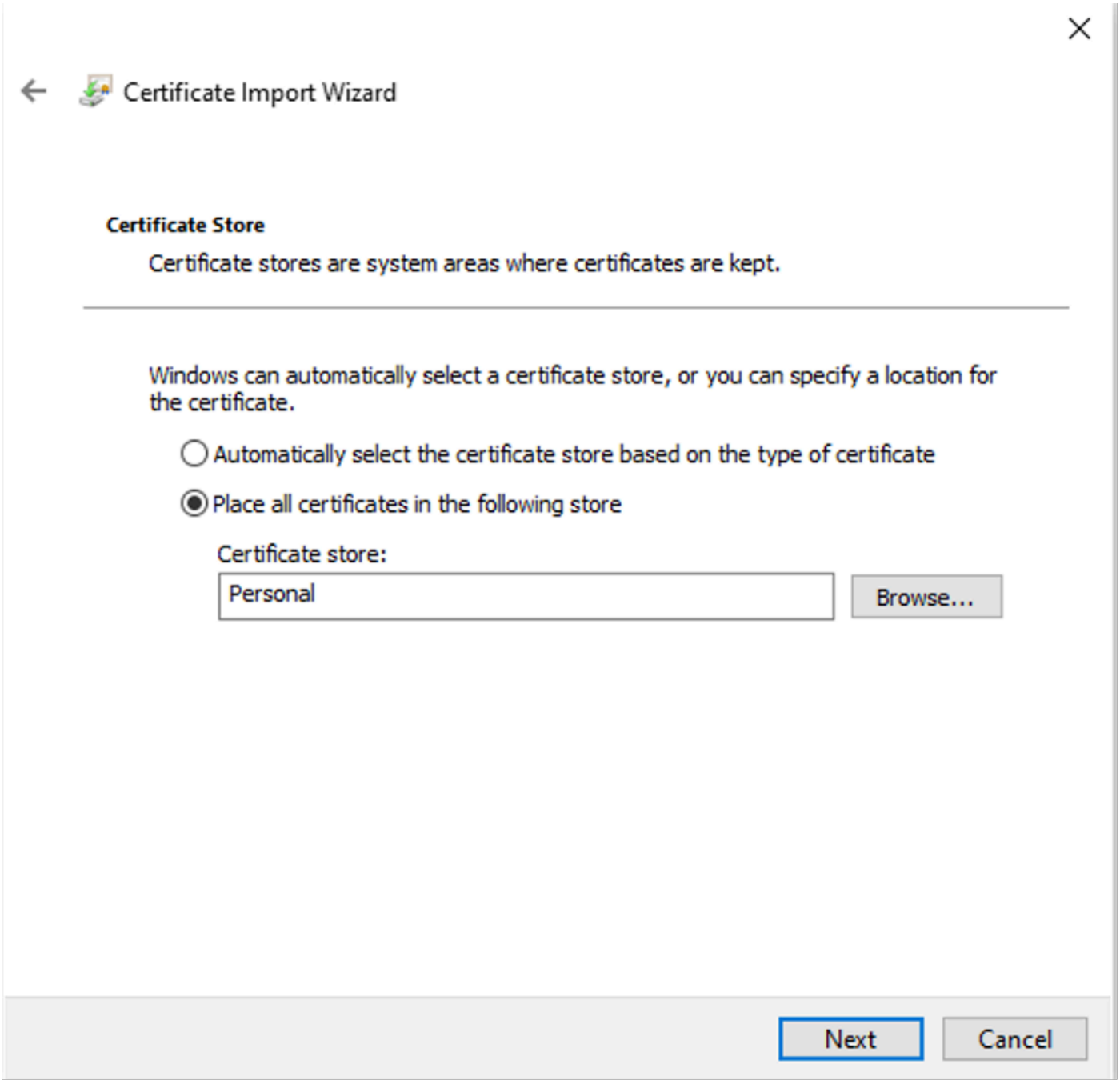
2.2. Review the certificates and determine their types (for example, Root CA, Intermediate CA, or Personal).

2.3. Move each **certificate** to the appropriate store:

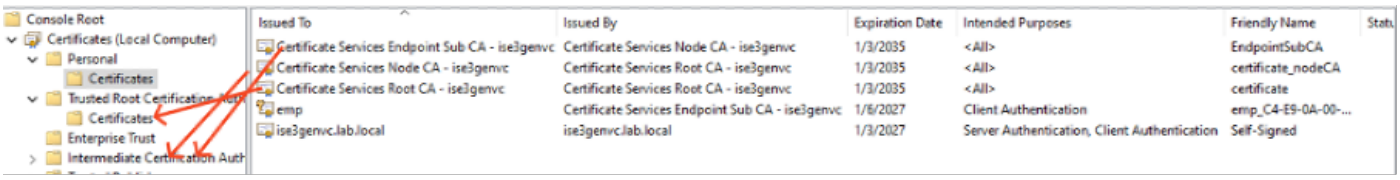
2.4. Root CA Certificates: Move to **Trusted Root Certification Authorities**.

2.5. Intermediate CA Certificates: Move to **Intermediate Certification Authorities**.

2.6. Personal Certificates: Leave in the **Personal folder**.



Storing Certificates in the Personal Folder

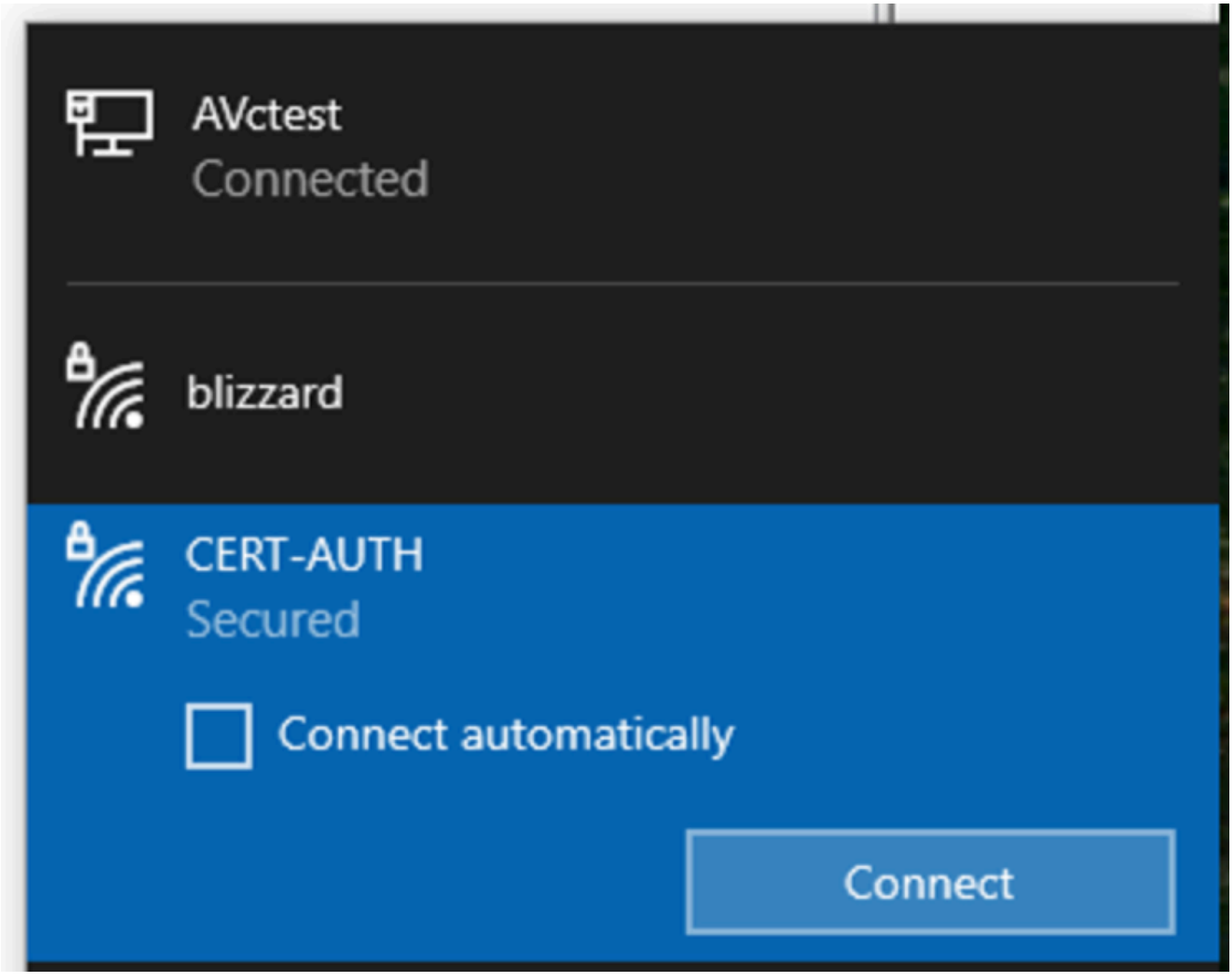


Moving Certificates in their Stores

Connecting the Windows Machine

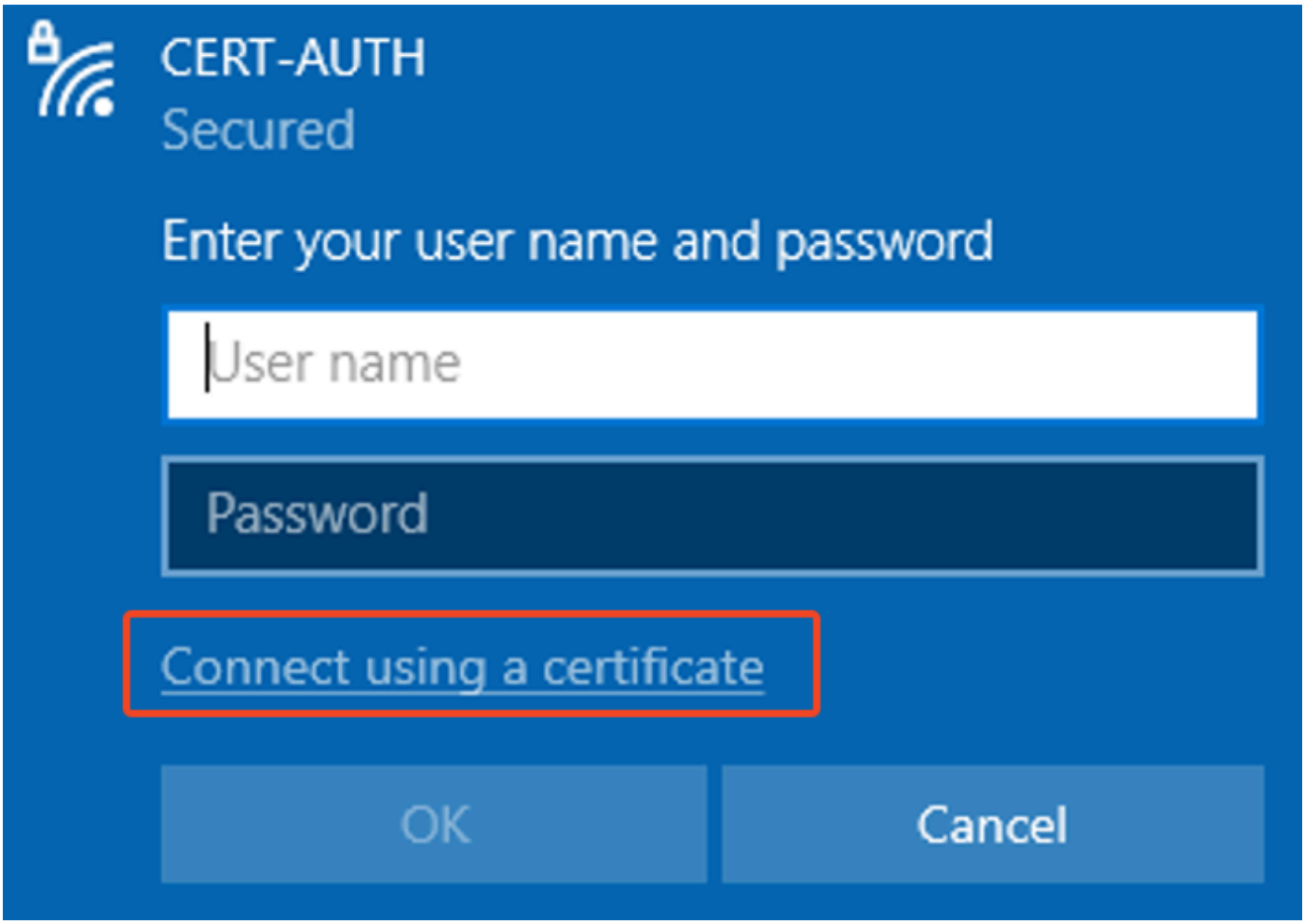
Once the certificates are moved to the correct stores, use these steps to connect to the WLAN:

1. Click the **network** icon in the system tray to view available wireless networks.
2. Find and click the **name** of the WLAN you wish to connect to.
3. Click **Connect** and proceed with any additional prompts to complete the connection process using your certificate for authentication.



Connecting to the Wireless Network

When prompted during the connection process to the WLAN, select the option to **Connect using a certificate**.



Using Certificate as Credential

This enables you to successfully connect to the wireless network using the certificate.

```
C:\>netsh wlan  show interface

There is 1 interface on the system:

    Name                   : Wi-Fi 3
    Description            : TP-Link Wireless USB Adapter
    GUID                   : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
    Physical address       : 24:2f:d0:da:a5:63
    State                  : connected
    SSID                   : CERT-AUTH
    BSSID                  : a4:88:73:9e:8d:af
    Network type           : Infrastructure
    Radio type             : 802.11ac
    Authentication         : WPA2-Enterprise
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 36
    Receive rate (Mbps)    : 360
    Transmit rate (Mbps)   : 360
    Signal                 : 100%
    Profile                : CERT-AUTH

    Hosted network status  : Not available


C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
    EAP type               : Microsoft: Smart Card or other certificate
```

Verify Wireless Profile

Verify

Verify that the WLAN is being broadcast by the WLC:

<#root>

```
POD6_9800#show wlan summ
Number of WLANs: 2
ID Profile Name SSID Status Security
-----------------------------------------------------------------------------------------------------------------
```

17

```
 CERT-AUTH
```

CERT-AUTH

```
 UP [WPA2][802.1x][AES]
```

Verify that the AP is up on the WLC:

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-------------------------------------------------------------------------------------------------
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

Ensure that the AP is broadcasting the WLAN:

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
------------------------
17 a488.739e.8da0

POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
------------------------
```

17

```
 a488.739e.8daf
```

Client connected using EAP-TLS:

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----------------------------------------------------------------------------------------------------
242f.d0da.a563 AP1 WLAN
```

17

```
 IP Learn 11ac
```

Dot1x

```
 Local

POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
```

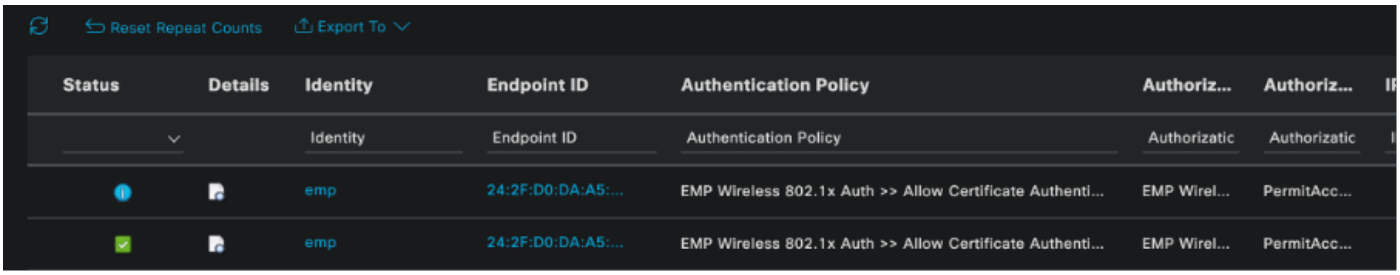
Wireless LAN Network Name (SSID): CERT-AUTH

BSSID : a488.739e.8daf

EAP Type : EAP-TLS

VLAN : 2124
Multicast VLAN : 0
VLAN : 2124

Cisco Radius ISE live logs:



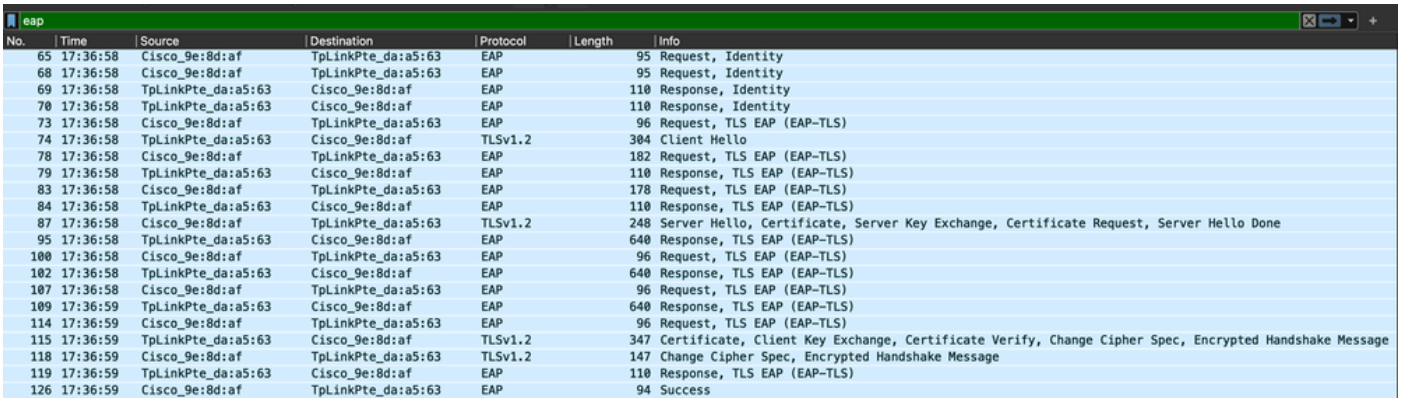
ISE Radius Live Logs

Detailed authentication type:



ISE Detailed Logs

WLC EPC Capture showing the EAP-TLS packets:



No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

WLC Capture Showing the EAP Transaction

- Packet number 87 corresponds to step 8 in the EAP-TLS Flow described at the beginning of the document.
- Packet number 115 corresponds to step 9 in the EAP-TLS Flow described at the beginning of the document.
- Packet number 118 corresponds to step 10 in the EAP-TLS Flow described at the beginning of the document.

Radio Active (RA) Trace Showing Client Connection: This RA trace is filtered to display a few of the relevant lines of the authentication transaction.

2025/01/08 11 58 20.816875191 {wncd_x_R0-2}{1} [ewlc-capwapmsg-sess] [15655] (debug) Encrypted DTLS message send. Dest IP 10.78.8.78[5256], length 499
2025/01/08 11 58 20.851392112 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/25, len 390
2025/01/08 11 58 20.871842938 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/25 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.872246323 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 20.881960763 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 204, EAP-Type = EAP-TLS
2025/01/08 11 58 20.882292551 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/26, len 663
2025/01/08 11 58 20.926204990 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/26 10.106.33.23 0, Access-Challenge, len 1135
2025/01/08 11 58 20.927390754 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 1012, EAP-Type = EAP-TLS
2025/01/08 11 58 20.935081108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 20.935405770 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/27, len 465
2025/01/08 11 58 20.938485635 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id

1812/27 10.106.33.23 0, Access-Challenge, len 1131
2025/01/08 11 58 20.939630108 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 1008, EAP-Type = EAP-TLS
2025/01/08 11 58 20.947417061 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 20.947722851 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/28, len 465
2025/01/08 11 58 20.949913199 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/28 10.106.33.23 0, Access-Challenge, len 275
2025/01/08 11 58 20.950432303 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 158, EAP-Type = EAP-TLS
2025/01/08 11 58 20.966862562 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.967209224 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/29, len 1961
2025/01/08 11 58 20.971337739 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/29 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.971708100 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 20.978742828 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.979081544 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/30, len 1961
2025/01/08 11 58 20.982535977 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/30 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.982907200 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 20.990141062 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 1492, EAP-Type = EAP-TLS
2025/01/08 11 58 20.990472026 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/31, len 1961
2025/01/08 11 58 20.994358525 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/31 10.106.33.23 0, Access-Challenge, len 123
2025/01/08 11 58 20.994722151 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 21.001735553 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 247, EAP-Type = EAP-TLS
2025/01/08 11 58 21.002076369 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/32, len 706
2025/01/08 11 58 21.013571608 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/32 10.106.33.23 0, Access-Challenge, len 174
2025/01/08 11 58 21.013987785 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Sent EAPOL packet - Version 3,EAPOL Type EAP, Payload Length 57, EAP-Type = EAP-TLS

2025/01/08 11 58 21.024429150 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Received EAPOL packet - Version 1,EAPOL Type EAP, Payload Length 6, EAP-Type = EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Send Access-Request to 10.106.33.23 1812 id 0/33, len 465
2025/01/08 11 58 21.057794929 {wncd_x_R0-2}{1} [radius] [15655] (info) RADIUS Received from id 1812/33 10.106.33.23 0, Access-Accept, len 324
2025/01/08 11 58 21.058149893 {wncd_x_R0-2}{1} [dot1x] [15655] (info) [242f.d0da.a563 capwap_90800005] Raised identity update event for eap method EAP-TLS

Troubleshoot

There are no specific troubleshooting steps for this issue beyond the typical Wireless 802.1x troubleshooting procedures:

1. Take Client RA trace debugs to check the authentication process.
2. Perform a WLC EPC capture to examine the packets between the client, WLC, and RADIUS server.
3. Check ISE live logs to verify that the request is matching the correct policy.
4. Verify on the Windows endpoint that the certificate is installed correctly and that the entire trust chain is present.

Related Information

- Certificate Provisioning Portal FAQs, Release 3.2
- Understand ISE Internal Certificate Authority Services
- Understand and Configure EAP-TLS with a WLC and ISE